Indoor/2.6x Zoom/Dual Streams PZ7131/PZ7132

NETWORK CAMERA

User's Manual

VIVOTEK
www.vivotek.com

IP Surveillance

Table of Contents

Overview

VIVOTEK PZ7131 (PoE) / 7132 (WLAN), equipped with a pan-focus 2.6x optical zoom lens, is a cost-effective pan/tilt/zoom network camera for indoor surveillance applications such as retail stores. It integrates a 2.6x motorized pan-focus zoom module, which can easily zoom in and out to view near or distant objects. With a 350-degree horizontal and 125-degree vertical range of capture, it effectively gives users a wide-area bird's view. With self-developed VIVOTEK VVTK-1000 SoC, the camera can simultaneously deliver dual video streams for real-time monitoring in either MJPEG or MPEG-4 format with different resolution. PZ7131 supports built-in IEEE 802.3af-compliant PoE (Power over Ethernet) and PZ7132 supports 802.11g wireless LAN connection, making installation easier and more cost-efficient. It comes with the free-bundled, multi-lingual 16-channel recording software, which helps users to set up a powerful surveillance system.

Read before use

The use of surveillance devices may be prohibited by law in your country. The Network Camera is not only a high-performance web-ready camera but also can be part of a flexible surveillance system. It is the user's responsibility to ensure that the operation of such devices is legal before installing this unit for its intended use.

It is important to first verify that all contents received are complete according to the Package contents listed below. Take notice of the warnings in Quick Installation Guide before the Network Camera is installed; then carefully read and follow the instructions in the Installation chapter to avoid damages due to faulty assembly and installation. This also ensures the product is used properly as intended.

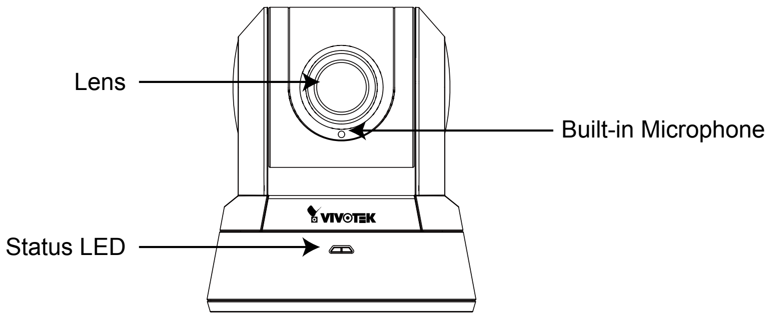
The Network Camera is a network device and its use should be straightforward for those who have basic network knowledge. It is designed for various applications including video sharing, general security/surveillance, etc. The Configuration chapter suggests ways to best utilize the Network Camera and ensure proper operations. For the creative and professional developers, the URL Commands of the Network Camera section serves to be a helpful reference to customize existing homepages or integrating with the current web server.

Package contents

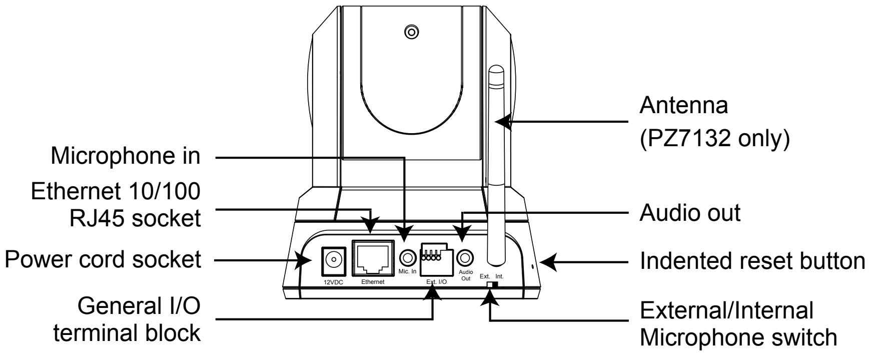
■ PZ7131 / PZ7132
■ Power adapter
■ Antenna (PZ7132 only)
■ Screws
■ Quick installation guide
■ Software CD
■ Warranty card
■ Ceiling mount brackets

Physical description

Front panel

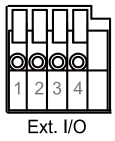


Rear panel



General I/O Terminal Block

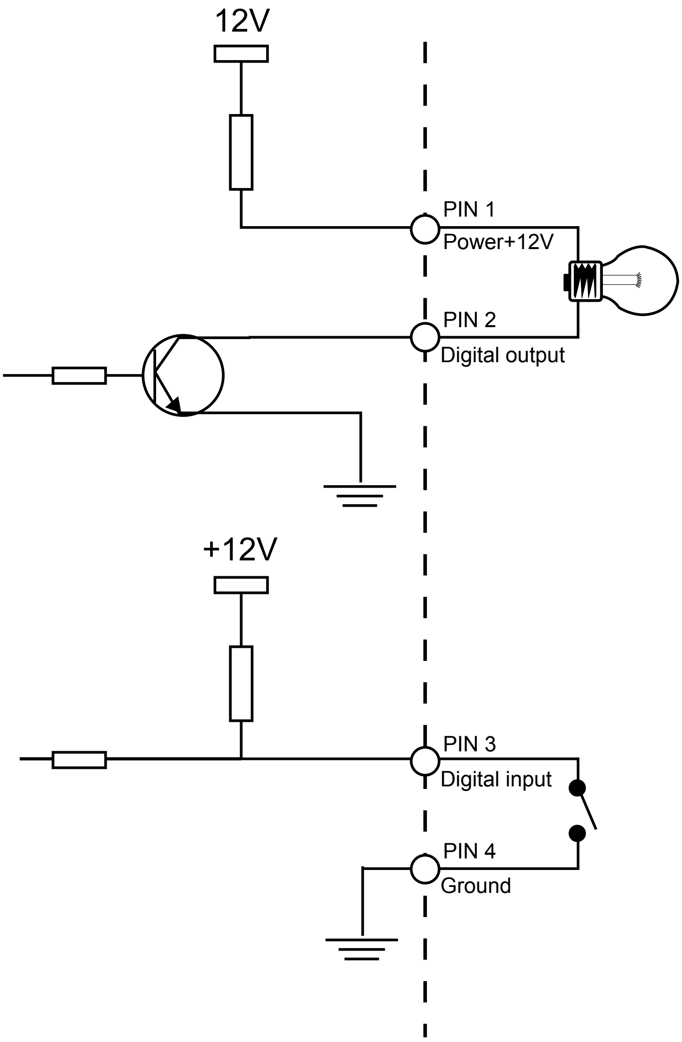
This Network Camera provides a general I/O terminal block which is used to connect external input / output devices. The pin definitions are described below.



Pin	Name	Specification	Remarks
1	Power	12VDC ± 5%, max. 1.5A	Max. rating 2A
2	Digital output	Max. 40VDC, max. 400mA, isolation 2kV	
3	Digital input	OPEN/Short-to-GND, isolation 2kV	Internal pull-up
4	Ground		

DI/DO Diagram

Pin 1~4 are used to connect with digital input and digital output devices. Refer to the following illustration for connection method.

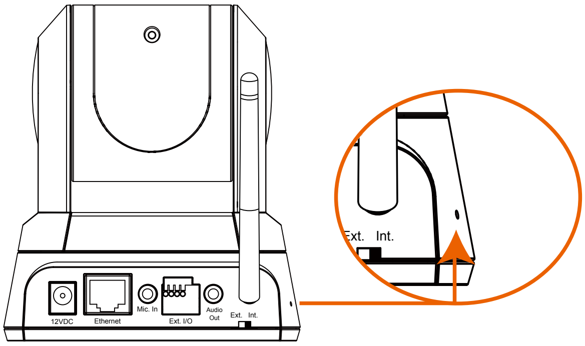


Status LED

The color of LED indicates the status of the Network Camera.

Status LED Color	Description
Blinking red	Power is being supplied to the Network Camera.
Steady green	The Network Camera is booting up.
Steady green with blinking red in between	The Network Camera is trying to obtain an IP address.
Steady green and red	An IP address is successfully assigned to the Network Camera.
Steady red with blinking green in between	The Network Camera is working.
Blinking red and green	During firmware upgrade

Hardware Reset



There is an indented reset button on the side panel of the Network Camera. It is used to reboot the Network Camera or restore the Network Camera to factory default. Sometimes rebooting the Network Camera could set the Network Camera back to normal state. If the problems remain after rebooted, restore the Network Camera to factory default and install again.

<u>Reset</u>: Press and release the indented reset button with a needle. Wait for the Network Camera to reboot.

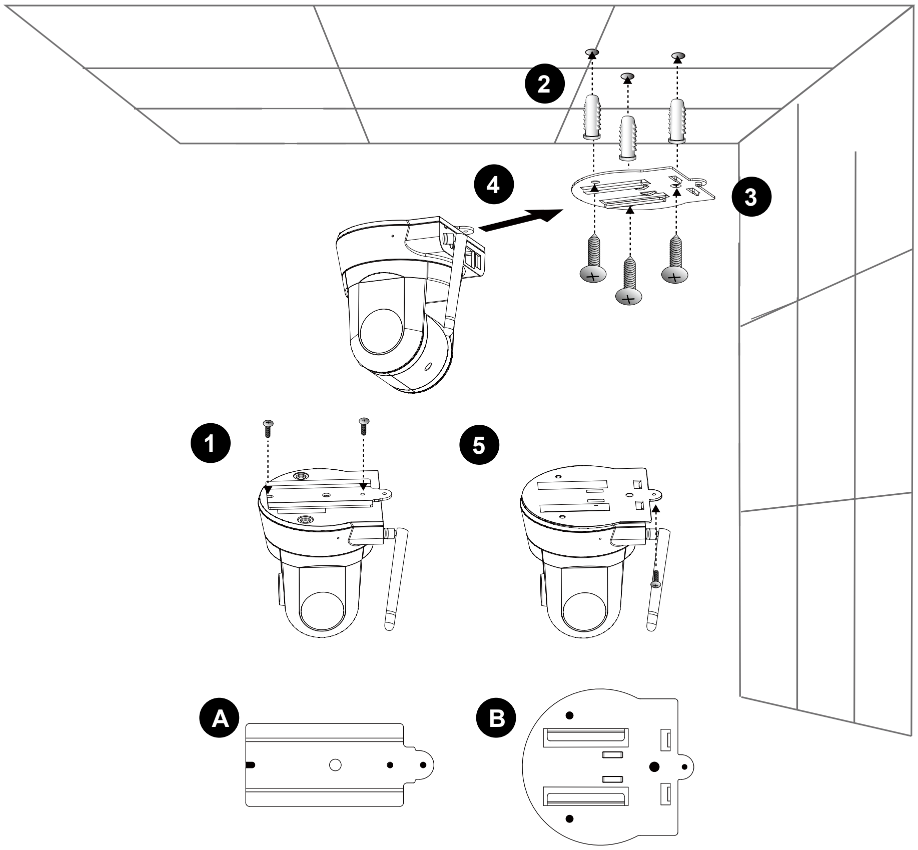
<u>Restore</u>: Press the indented reset button continuously for over 5 seconds until the status LED rapidly blinks red and green simultaneously. Note that all settings will be restored to factory default.

Installation

Hardware installation

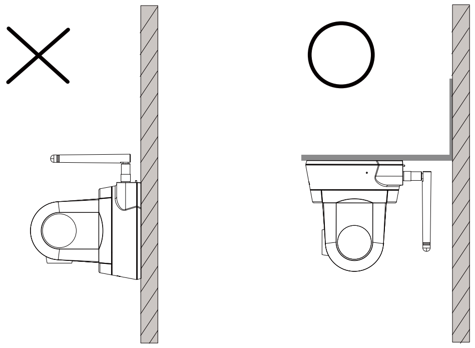
Follow the steps below to install the Network Camera to the ceiling:

1. Attach ceiling mount bracket A to the Network Camera and secure it with two small screws.
2. Drill three pilot holes into the ceiling; hammer the plastic anchors into the holes.
3. Fasten ceiling mount bracket B to the ceiling with three screws.
4. Slide the Network Camera into ceiling mount bracket B.
5. Secure ceiling mount bracket A and B with a small screw.



NOTE

► *If you want to install the Network Camera on the wall, please use the wall mount bracket (optional, not included in the package).*

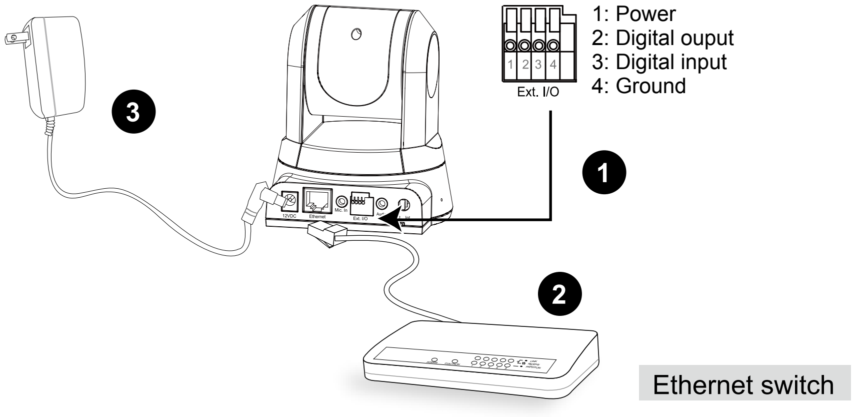


Network deployment

Setup the Network Camera over the Internet

This section explains how to configure the Network Camera to Internet connection.

1. If you have external devices such as sensors and alarms, make connection from general I/O terminal block.
2. Connect the camera to a switch via Ethernet cable.
3. Connect the supplied power cable from the Network Camera to a power outlet.

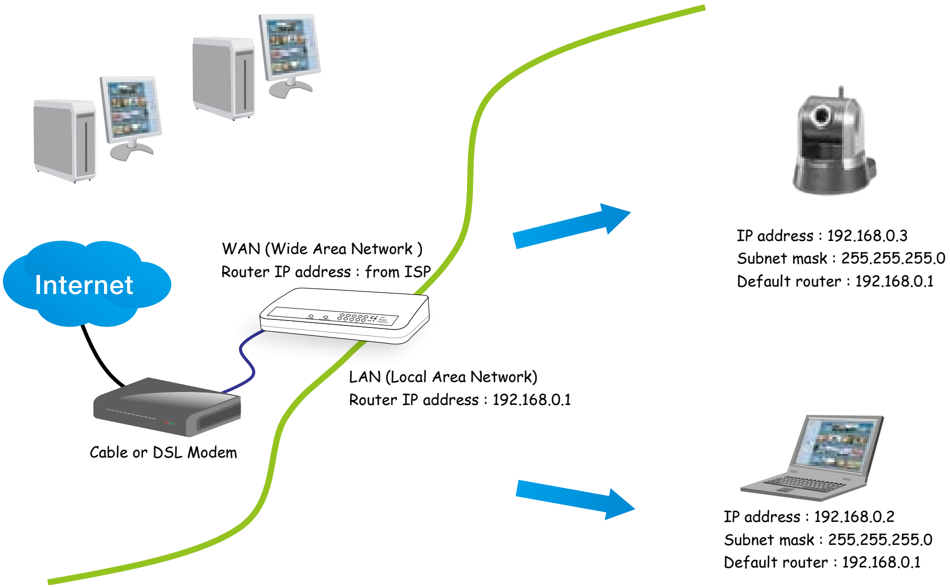


There are several ways to setup the Network Camera over the Internet. The first way is to setup the Network Camera behind a router. The second way is to utilize a static IP. The third way is to use PPPoE.

Internet connection via a router

Before setting up the Network Camera over the Internet, make sure you have a router and follow the steps below.

1. Connect your Network Camera behind a router, the Internet environment is illustrated as below. About how to get your IP address, please refer to Software installation on page 12 for details.


Internet
WAN (Wide Area Network)
Router IP address : from ISP
LAN (Local Area Network)
Router IP address : 192.168.0.1
Cable or DSL Modem
IP address : 192.168.0.3
Subnet mask : 255.255.255.0
Default router : 192.168.0.1
IP address : 192.168.0.2
Subnet mask : 255.255.255.0
Default router : 192.168.0.1

2. In this case, if the Local Area Network (LAN) IP address of your Network Camera is 192.168.0.3, please forward the following ports for the Network Camera on the router.

■ HTTP port
■ RTSP port
■ RTP port for audio
■ RTCP port for audio
■ RTP port for video
■ RTCP port for video

If you have changed the port numbers on the Network page, please open the ports accordingly on your router. For information on how to forward ports on the router, please refer to the user's manual of your router.

3. Find out the public IP address of your router provided by your ISP (Internet Service Provider). Use the public IP and the secondary HTTP port to access the Network Camera from the Internet. Please refer to Network Type on page 33 for details.

Internet connection with static IP

Choose this connection type if you are required to use a static IP for the Network Camera. Please refer to LAN on page 33 for details.

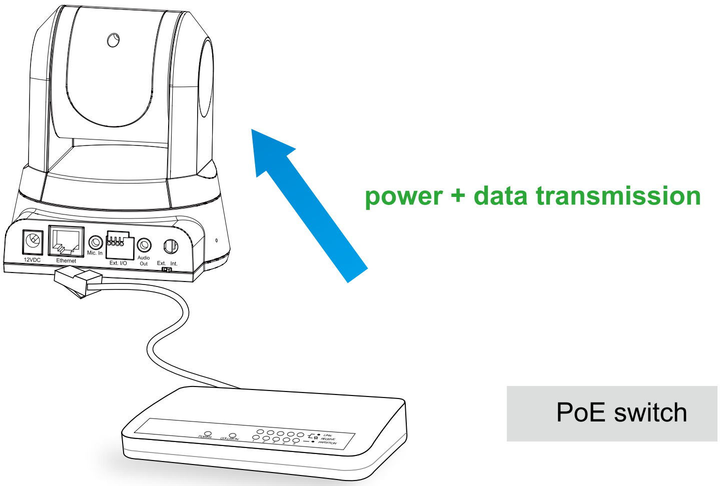
Internet connection via PPPoE (Point-to-Point over Ethernet)

Choose this connection type if you are connected to the Internet via a DSL Line. Please refer to PPPoE on page 34 for details.

Set up the Network Camera through Power over Ethernet (PoE) (PZ7131 only)

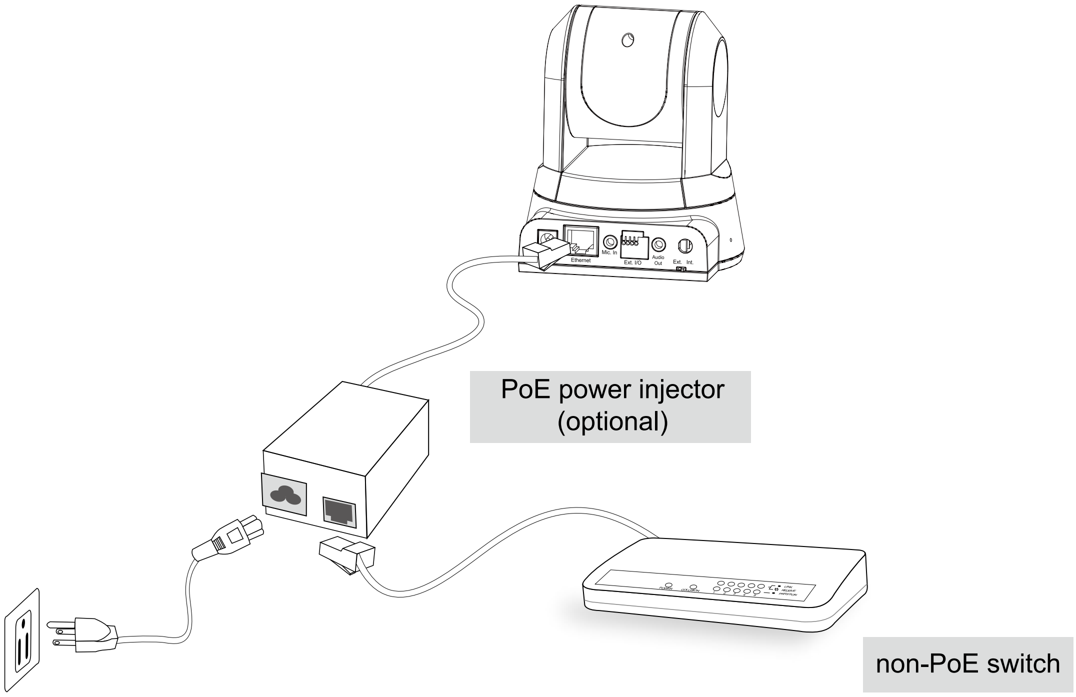
When using a PoE-enabled switch

The Network Camera is PoE-compliant, which allows it to be powered via a single Ethernet cable. If your switch/router supports PoE, refer to the following illustration to connect the Network Camera to a PoE-enabled switch/router via an Ethernet cable.



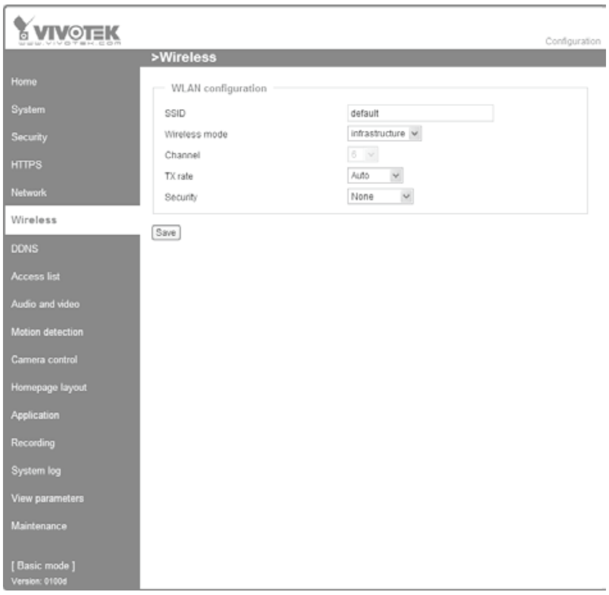
When using a non-PoE switch

If your switch/router does not support PoE, use a PoE power injector (optional) to connect between the Network Camera and a non-PoE switch/router.



Set up the Network Camera through Wireless Connection (PZ7132 only)

1. Check the SSID currently set on your wireless access point (AP).
2. Go to PZ7132's Configuration > Advanced mode > Wireless.
3. Type in the SSID consistent with the setting on your AP.
4. Select the Wireless mode as "Infrastructure".
5. Click **Save**. The Network Camera starts to reboot.

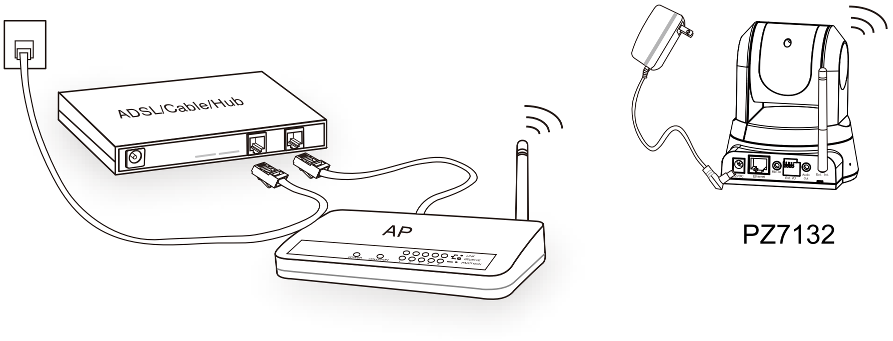


>Wireless

WLAN configuration

SSID: default
Wireless mode: infrastructure
Channel: 6
TX rate: Auto
Security: None

6. Wait for the live image is reloaded to your browser. Then, unplug the power cable and Ethernet cable from the Network Camera.
7. Replug the power cable to the camera. The Network Camera now operates in wireless mode.



NOTE

► *SSID, abbreviated from Service Set Identifier, is the name assigned to the wireless network. The PZ7132's factory SSID setting is set to "default".*

► *Select "Ad-Hoc" wireless mode if you want the PZ7132 to communicate without using an AP or wireless router.*

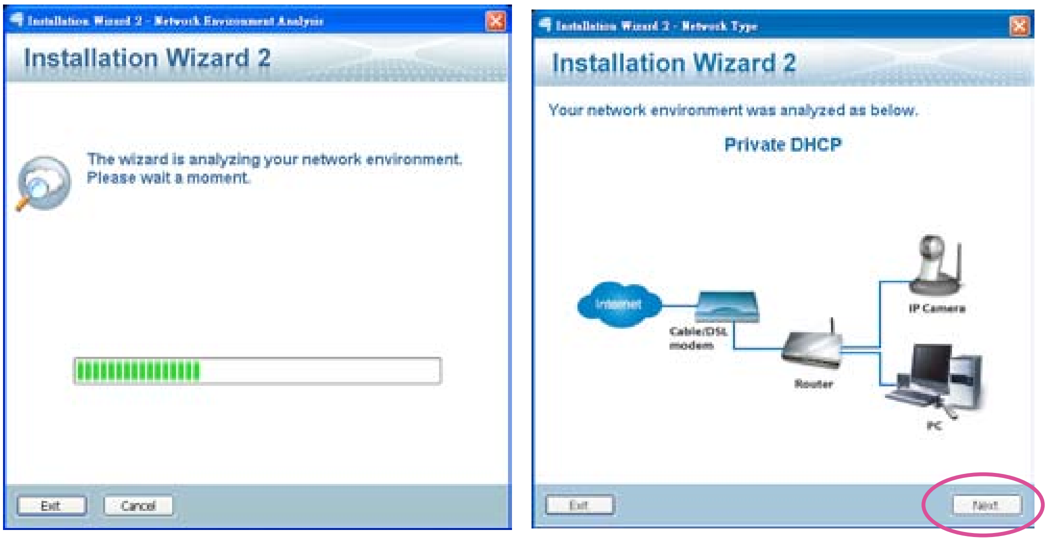
► *For detailed information about wireless connection, please refer to Wireless LAN on page 44.*

Software installation

Installation Wizard 2 (IW2), free-bundled software packaged in the product CD, helps to set up your Network Camera in LAN.

1. Install the IW2 under the Software Utility directory from the software CD.
   Double click the IW2 shortcut on your desktop to launch the program.

2. The program will conduct analyses on your network environment.
   After your network environment is analyzed, please click Next to continue the program.



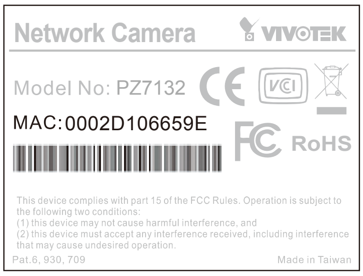
The wizard is analyzing your network environment.
Please wait a moment.

Your network environment was analyzed as below.

Private DHCP

3. The program will search all VIVOTEK devices in the same LAN.

4. After searching, the main installer window will pop up. Click on the MAC and model name which match the product label on your device to connect to the Network Camera via the Internet Explorer.



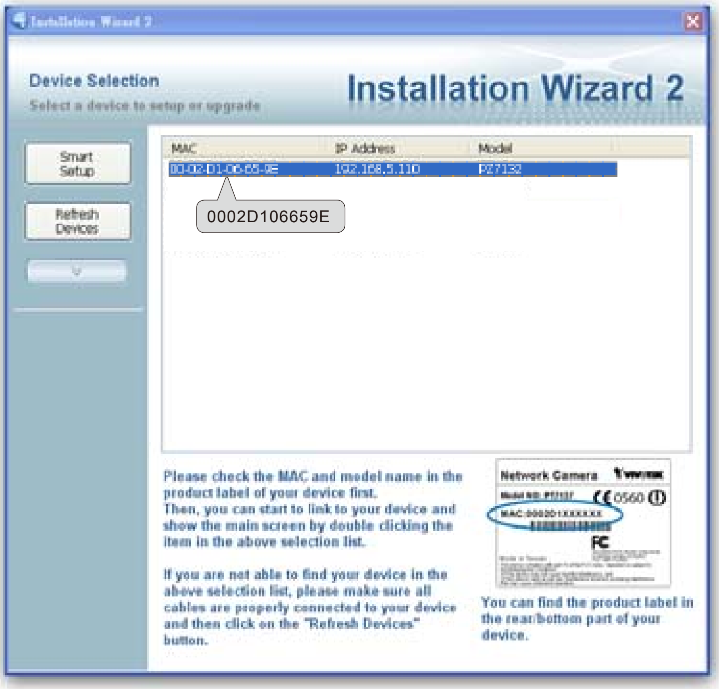
Model No: PZ7132

MAC: 0002D106659E

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:
(1) this device may not cause harmful interference, and
(2) this device must accept any interference received, including interference that may cause undesired operation.

Pat.6, 930, 709

Made in Taiwan



Device Selection
Select a device to setup or upgrade

MAC	IP Address	Model
00-02-D1-06-65-9E	192.168.5.110	PZ7132

Please check the MAC and model name in the product label of your device first.
Then, you can start to link to your device and show the main screen by double clicking the item in the above selection list.

If you are not able to find your device in the above selection list, please make sure all cables are properly connected to your device and then click on the "Refresh Devices" button.

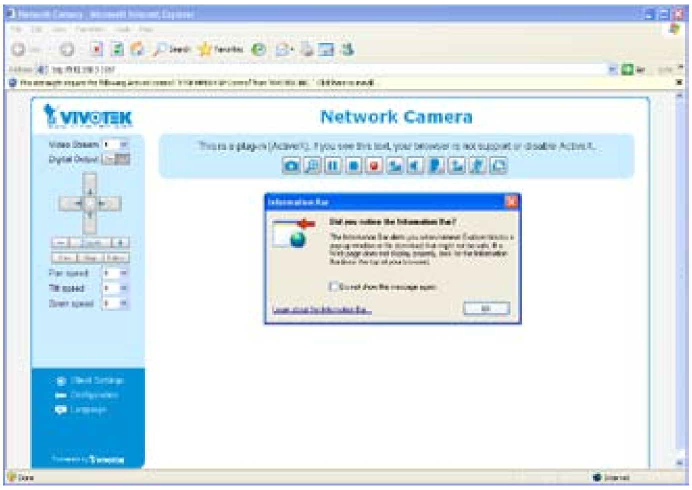
You can find the product label in the rear/bottom part of your device.

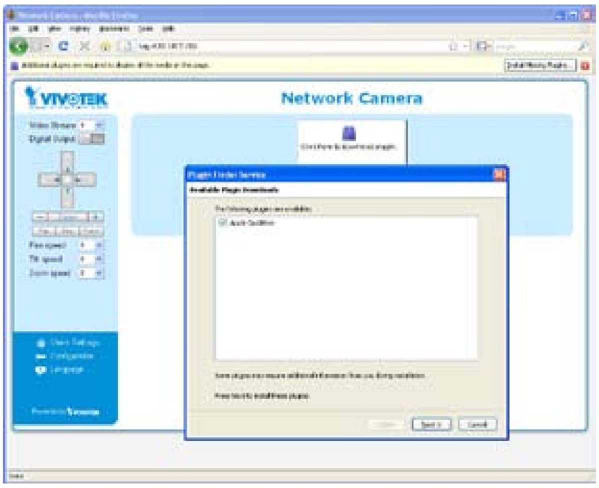
Accessing the Network Camera

This chapter explains how to access the Network Camera through web browsers, RTSP players, 3GPP-compatible mobile devices, and VIVOTEK recording software.

Using web browsers

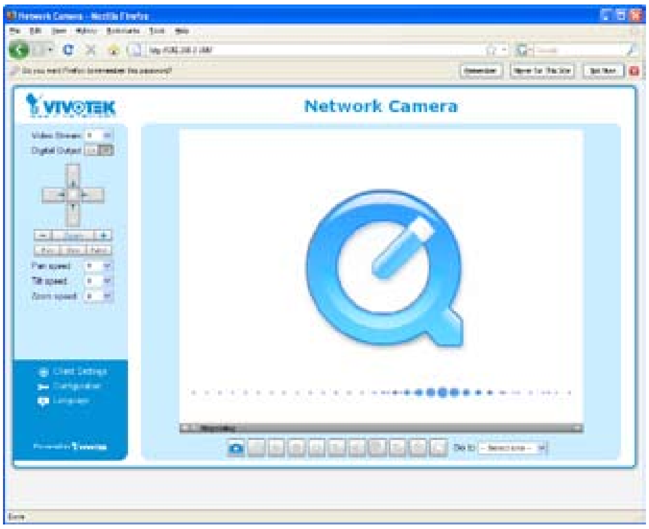
Make use of Installation Wizard 2 (IW2) to access to the Network Cameras in LAN.
If your network environment is not in LAN, follow the steps to access the Network Camera:
1. Launch your web browser (ex. Microsoft® Internet Explorer, Mozilla Firefox or Netscape).
2. Enter the IP address of the Network Camera in the address field. Press **Enter**.
3. The live video will be displayed in your web browser.
4. If it is the first time for you to install VIVOTEK's network camera, some information bar will pop up as below. Follow the instruction to install required plug-in on your computer.

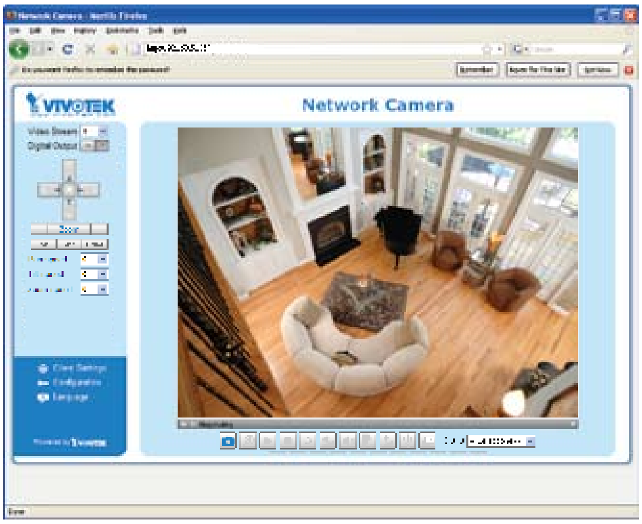




NOTE

► *For Mozilla Firefox or Netscape users, your browser will use Quick Time to stream the live video. If you don't have Quick Time on your computer, please download it first, and then launch the web browser.*

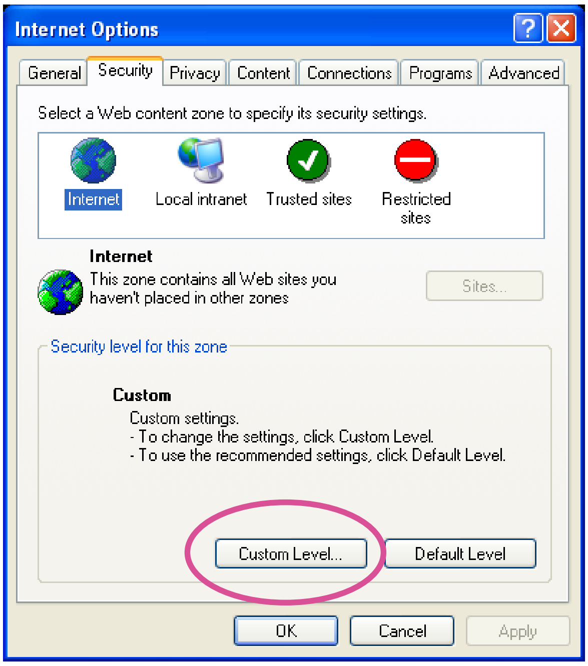




► *By default, the Network Camera is not password-protected. To prevent unauthorized accesses, it is highly recommended to set a password for the Network Camera.*
For more information about how to enable password protection, please refer to Security on page 27.

► *If you see a dialog box indicating that your security settings prohibit running ActiveX® Controls, please enable your ActiveX® Controls for your browser.*

1. Choose Tools > Internet Options > Security > Custom Level.



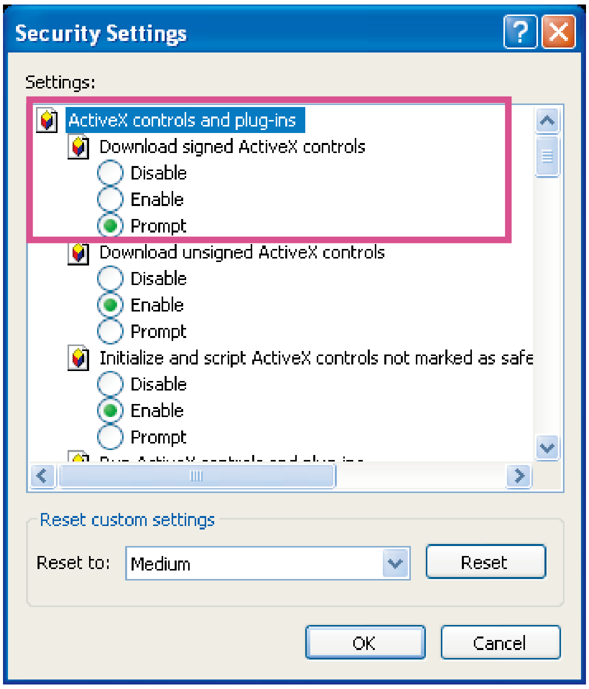
Select a Web content zone to specify its security settings.

Internet
This zone contains all Web sites you haven't placed in other zones

Security level for this zone

Custom
Custom settings.
- To change the settings, click Custom Level.
- To use the recommended settings, click Default Level.

2. Look for Download signed ActiveX® controls; select Enable or Prompt. Click ***OK****.*



Settings:

ActiveX controls and plug-ins
Download signed ActiveX controls
○ Disable
○ Enable
● Prompt
Download unsigned ActiveX controls
○ Disable
● Enable
○ Prompt
Initialize and script ActiveX controls not marked as safe
○ Disable
● Enable
○ Prompt

Reset custom settings
Reset to: Medium

3. Refresh your web browser, and then install the Active X®. Follow the instructions to finish installation.

Using RTSP players

To view the MPEG-4 streaming media using RTSP players, you can use one of the following players that support RTSP streaming.

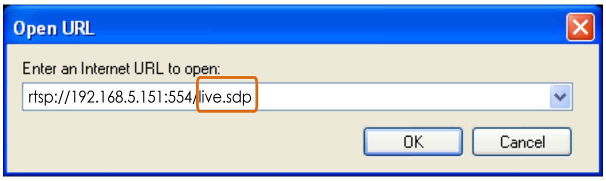
Quick Time Player

Real Player

1. Launch a RTSP player.
2. Choose File > Open URL. An URL dialog box will pop up.
3. The format is rtsp://<ip address>:<rtsp port>/<RTSP streaming access name for stream1 or stream2>

   As most ISP and players only support port number 554 to allow RTSP streaming to go through, please set the RTSP port to 554. For more information, please refer to RTSP Streaming on page 42.

   For example:



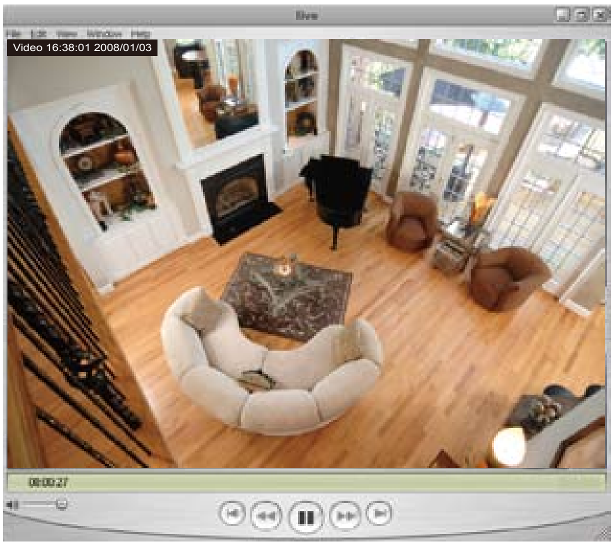
Open URL

Enter an Internet URL to open:

rtsp://192.168.5.151:554/live.sdp

4. The live video will be displayed in your player.

   For more information on how to configure RTSP access name, please refer to RTSP Streaming on page 42 for details.



Using 3GPP-compatible mobile devices

To view the streaming media through 3GPP-compatible mobile devices, make sure the Network Camera can be accessed from the Internet. For more information on how to set up the Network Camera over the Internet, please refer to Setup the Network Camera over the Internet on page 8.

To utilize this feature, please check the following settings on your Network Camera:

1. Because most players on 3GPP mobile phones do not support RTSP authentication, make sure the authentication mode of RTSP streaming is set to disable.
   For more information, please refer to RTSP Streaming on page 42.

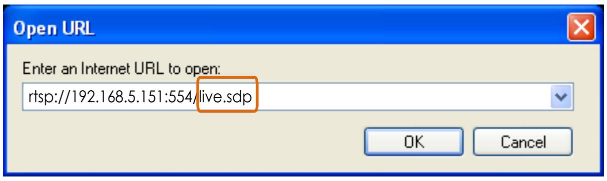
2. As the 3G network bandwidth is limited, you can't use large video size. Please set the video and audio streaming parameters as listed below.
   For more information, please refer to Audio and video on page 52.

Video Mode	MPEG-4
Frame size	176 x 144
Maximum frame rate	5 fps
Intra frame period	1S
Video quality (Constant bit rate)	40kbps
Audio type (GSM-AMR)	12.2kbps

3. As most ISP and players only support port number 554 to allow RTSP streaming to go through, please set the RTSP port to 554. For more information, please refer to RTSP Streaming on page 42.

4. Launch the players on 3GPP-compatible mobile devices (ex. Real Player).

5. Type the URL commands in the player.
   The format is rtsp://<public ip address of your camera>:<rtsp port>/<RTSP streaming access name for stream1 or stream2>.
   For example:



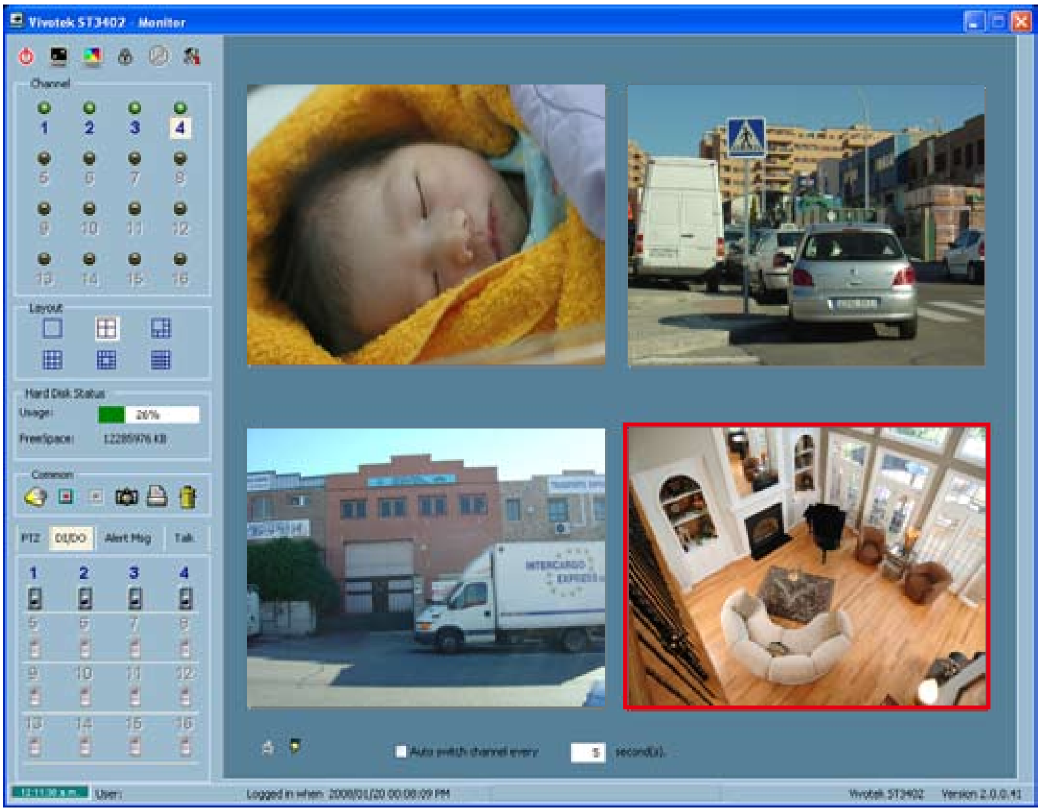
Open URL

Enter an Internet URL to open:

rtsp://192.168.5.151:554/live.sdp

Using VIVOTEK recording software

The product software CD also contains recording software, allowing simultaneous monitoring and video recording for multiple Network Cameras. Please install the recording software; then launch the program to add the Network Camera to the Channel list. For detailed information about how to use the recording software, please refer to the user's manual of the software or download it at http://www.vivotek.com.



Usage: 26%

FreeSpace: 12285976 KB

□ Auto switch channel every 5 second(s).

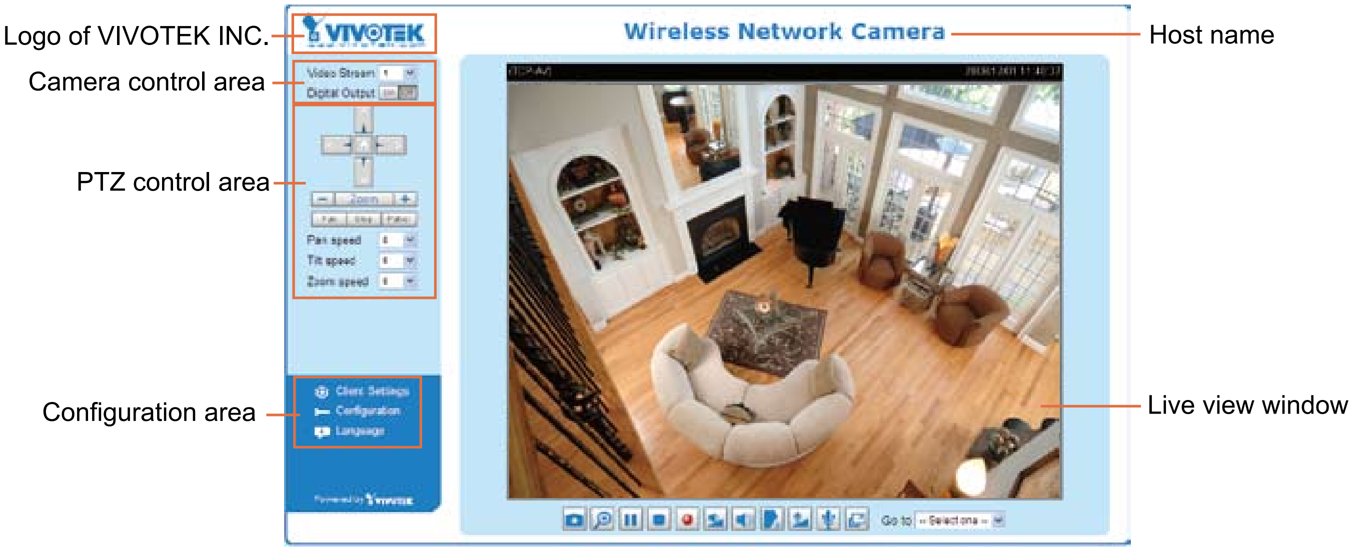
User:

Logged in when: 2008/01/20 00:08:09 PM

Vivotek ST3402 Version 2.0.0.41

Main Page

This chapter explains the layout of the main page. It is composed of the following sections: Logo of VIVOTEK INC., Host name, Camera control panel, Menu, and Live video window.



Logo of VIVOTEK INC.

Click this logo to visit VIVOTEK website.

Host name

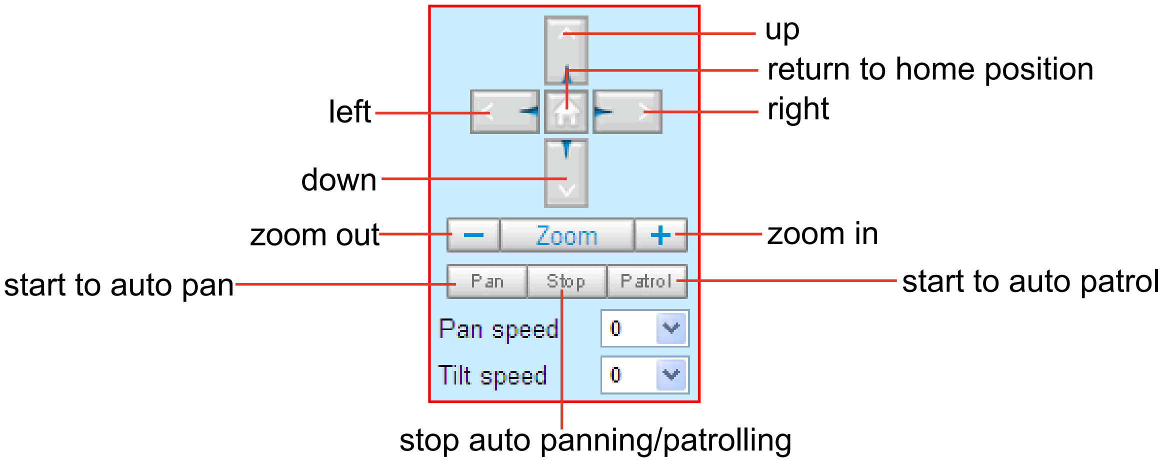
The host name can be customized to fit your needs. For more information, please refer to System on page 25.

Camera control area

Video Stream: This Network Camera supports MJPEG or MPEG-4 dual streams simultaneously. You can select either one for live viewing.

Digital Output: Click to turn on or off the digital output device.

PTZ control panel



Pan: Click this button to start the auto pan. When the current position is Home or on the left side of Home, the camera starts panning from the current position to the left-most position, then to the right-most position, and finally backward to the original position. When the current position is on the right side of Home, the camera starts panning from the current position to the right-most position, then to the left-most position, and finally backward to the original position.

Stop: Click this button to stop the auto Pan and auto Patrol function.

Patrol: Once the Administrator has determined the preset positions, click this button to command the camera to patrol among those positions on the Patrol List. After one patrol cycle, the camera returns to the original position. For more information, please refer to Camera control of Configuration on page 60.

Pan /Tilt speed: Adjust the speed of pan/ tilt.

Pan speed	Tilt speed	
-5	-5	Slower
-4	-4	↑
-3	-3	
-2	-2	
-1	-1	
0	0	
1	1	
2	2	
3	3	
4	4	↓
5	5	Faster

Configuration area

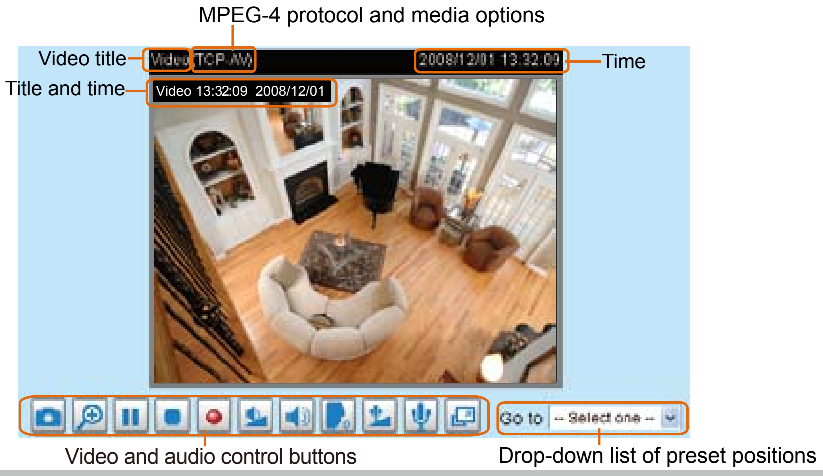
Client Settings: Click this button to access the client setting page. For more information, please refer to Client Settings on page 22.

Configuration: Click this button to access the configuration page of Network Camera. It is suggested that a password is applied to the Network Camera so that only the administrator can configure the Network Camera. For more information, please refer to Configuration on page 24.

Language: Click this button to choose a language for the user interface. Language options are available in: English, Deutsch, Español, Français, Italiano, 日本語, Português, 簡体中文 and 繁體中文.

Live Video Window

■ The following window is displayed when the video mode is set to MPEG-4:


MPEG-4 protocol and media options
Video title
Video
TCP-AV
2008/12/01 13:32:09
Time
Title and time
Video 13:32:09 2008/12/01
Go to
-- Select one --
Video and audio control buttons
Drop-down list of preset positions

Video title: The video title can be configured. For more information, please refer to Video settings on page 52.

MPEG-4 protocol and media options: The transmission protocol and media options for MPEG-4 video streaming. For further configuration, please refer to Client Settings on page 22.

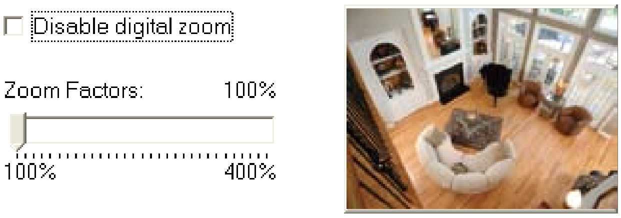
Time: Display the current time. For further configuration, please refer to Video settings on page 52.

Title and time: Video title and time can be stamped on the streaming video. For further configuration, please refer to Video settings on page 52.

Video and audio control buttons: Depending on the Network Camera model and Network Camera configuration, some buttons may not be available.

Snapshot: Click this button to capture and save still images. The captured images will be displayed in a pop-up window. Right-click the image and choose **Save Picture As** to save it in JPEG (*.jpg) or BMP (*.bmp) format.

Digital zoom: Click and uncheck **Disable digital zoom** to enable the zoom operation. The navigation screen indicates which part of the image is being magnified. To control the zoom level, drag the slider bar. To move to a different area you want to magnify, drag the navigation screen.



☐ Disable digital zoom

Zoom Factors: 100%

100% 400%

⏸ Pause: Pause the transmission of streaming media. The button becomes ▶ Resume button after clicking the Pause button.

■ Stop: Stop the transmission of streaming media. Click the ▶ Resume button to continue transmission.

● Start MP4 recording: Click this button to record video clips in MP4 file format to your computer. Press the ■ Stop MP4 recording button to end recording. When you quit the web browser, video recording stops accordingly. To specify the storage destination and the file name, please refer to MP4 Saving Options on page 23 for details.

Volume: When the 🔊 Mute function is not activated, move the slider bar to adjust the volume at local computer.

🔊 Mute: Turn off the volume at local computer. The button becomes Audio on button after clicking the Mute button.

Talk: Click this button to talk to people around the Network Camera. Audio will come out from the external speaker connected to the Network Camera. Click this button again to stop talk.

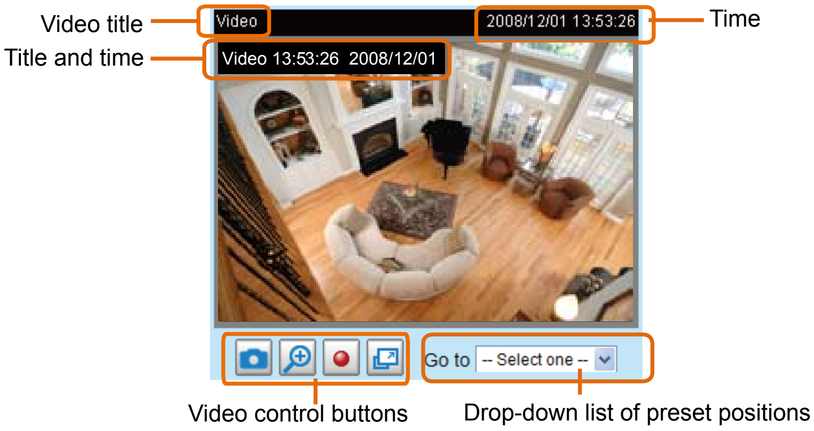
Mic Volume: When the Mute function is not activated, move the slider bar to adjust the microphone volume at local computer.

Mute: Turn off the Mic volume at local computer. The button becomes Mic on button after clicking the Mute button.

Full Screen: Click this button to switch to full screen mode. Press “Esc” key to switch back to normal mode.

Go to: Once the Administrator has determined the preset positions; you can aim the camera using this control. For more information, please refer to Camera control of Configuration on page 60.

■ The following window is displayed when the video mode is set to MJPEG:



Video title: The video title can be configured. For more information, please refer to Video settings on page 52.

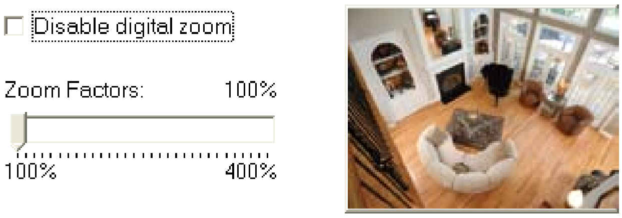
Time: Display the current time. For more information, please refer to Video settings on page 52.

Title and time: Video title and time can be stamped on the streaming video. For more information, please refer to Video settings on page 52.

Video and audio control buttons: Depending on the Network Camera model and Network Camera configuration, some buttons may not be available.

Snapshot: Click this button to capture and save still images. The captured images will be displayed in a pop-up window. Right-click the image and choose **Save Picture As** to save it in JPEG (*.jpg) or BMP (*.bmp) format.

Digital zoom: Click and uncheck Disable digital zoom to enable the zoom operation. The navigation screen indicates which part of the image is being magnified. To control the zoom level, drag the slider bar. To move to a different area you want to magnify, drag the navigation screen.


□ Disable digital zoom

Zoom Factors: 100%

Start MP4 recording: Click this button to record video clips in MP4 file format to your computer. Press the Stop MP4 recording button to end recording. When you quit the web browser, video recording stops accordingly. To specify the storage destination and the file name, please refer to MP4 Saving Options on page 23 for details.

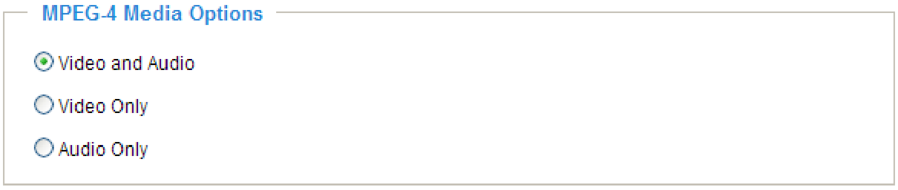
Full Screen: Click this button to switch to full screen mode. Press “Esc” key to switch back to normal mode.

Go to: Once the Administrator has determined the preset positions; you can aim the camera using this control. For more information, please refer to Camera control of Configuration on page 60.

Client Settings

This chapter explains how to select the stream transmission mode and saving options at local computer. When completed with the settings on this page, click **Save** on the page bottom to take effect.

MPEG-4 Media Options

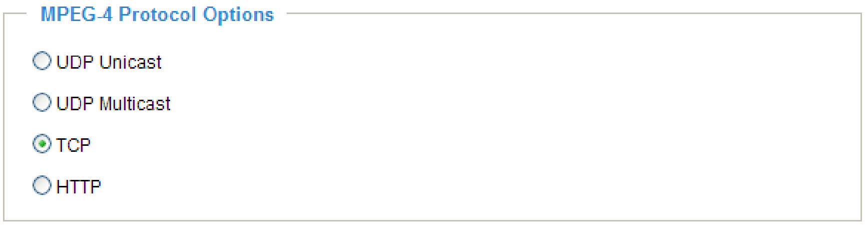


MPEG-4 Media Options

● Video and Audio
○ Video Only
○ Audio Only

Select to stream video or audio data. This works only when the video mode is set to MPEG-4.

MPEG-4 Protocol Options



MPEG-4 Protocol Options

○ UDP Unicast
○ UDP Multicast
● TCP
○ HTTP

Depending on your network environment, there are four transmission modes of MPEG-4 streaming:

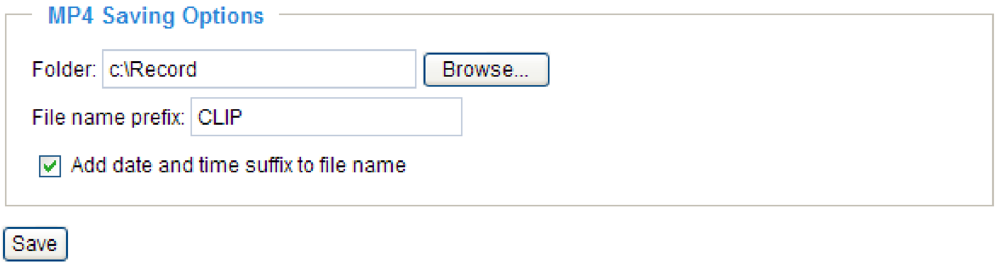
UDP unicast: This protocol allows for more real-time audio and video streams. However, network packets may be lost due to network burst traffic and images may be broken. Activate UDP connection when occasions require time-sensitive responses and the video quality is less important. Note that each unicast client connecting to the server takes up additional bandwidth and the Network Camera allows up to ten simultaneous accesses.

UDP multicast: This protocol allows multicast-enabled routers to forward network packets to all clients requesting streaming media. This helps to reduce the network transmission load of the Network Camera while serving multiple clients at the same time. Note that to utilize this feature, the Network Camera must be configured to enable multicast streaming at the same time. For more information, see RTSP Streaming on page 34.

TCP: This protocol guarantees the complete delivery of streaming data and thus provides better video quality. Nevertheless, the downside with this protocol is that its real-time effect is not as good as that of the UDP protocol.

HTTP: This protocol allows the same quality as TCP protocol and you don’t need to open specific port for streaming under some network environments. Users inside a firewall can utilize this protocol to allow streaming data to come through.

MP4 Saving Options



MP4 Saving Options

Folder: c:\Record

File name prefix: CLIP

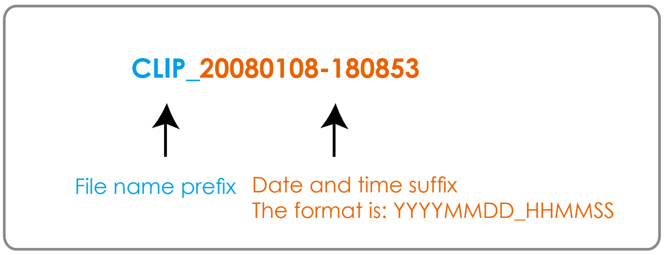
☑ Add date and time suffix to file name

Users can record the live video as they are watching it by clicking ● Start MP4 Recording on the main page. Here, you can specify the storage destination and file name.

Folder: Specify a storage destination for the recorded video files.

File Name Prefix: Enter the text that will be put in front of the video file name.

Add date and time suffix to the file name: Select this option to add date and time to the file name suffix.



Configuration

Click **Configuration** on the main page will enter the camera setting pages. Note that only Administrators can access the configuration page.

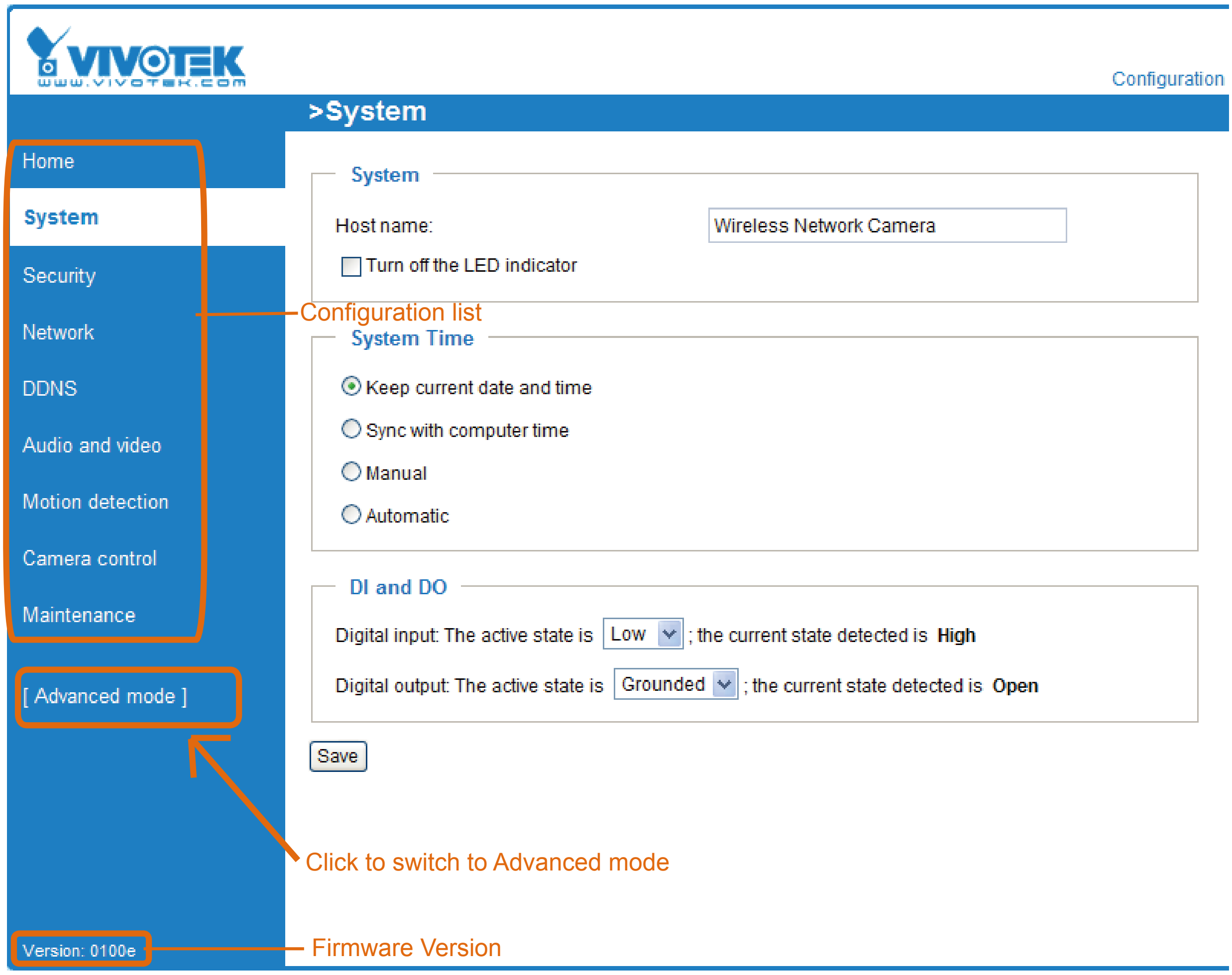
VIVOTEK offers an easy-to-use user interface that helps you setup your network camera without much efforts. To simplify the setting procedure, VIVOTEK designs two kinds of user inferface--advanced mode for professional users and basic mode for entry-level users. Some advanced functions (HTTPS/ Wireless/ Access list/ Homepage layout/ Application/ Recording/ System log/ View parameters) won't be displayed in basic mode.

If you want to set up advanced functions, please click **[Advanced mode]** on the bottom of the configuration list to quickly switch to Advanced mode.

Another smart design to keep this user interface neat and easy to configure is that the detailed information will be hidden unless you click on the function item. When you click on the first function item, the detailed information of the first function item will be displayed; when you click on the second function item, the detailed information of the second function item will be displayed and that of the first function item will roll up simultaneously.

Following is the interface of Basic mode and Advanced mode:

Basic mode



System

Host name: Wireless Network Camera

□ Turn off the LED indicator

System Time

● Keep current date and time

○ Sync with computer time

○ Manual

○ Automatic

DI and DO

Digital input: The active state is Low ; the current state detected is **High**

Digital output: The active state is Grounded ; the current state detected is **Open**

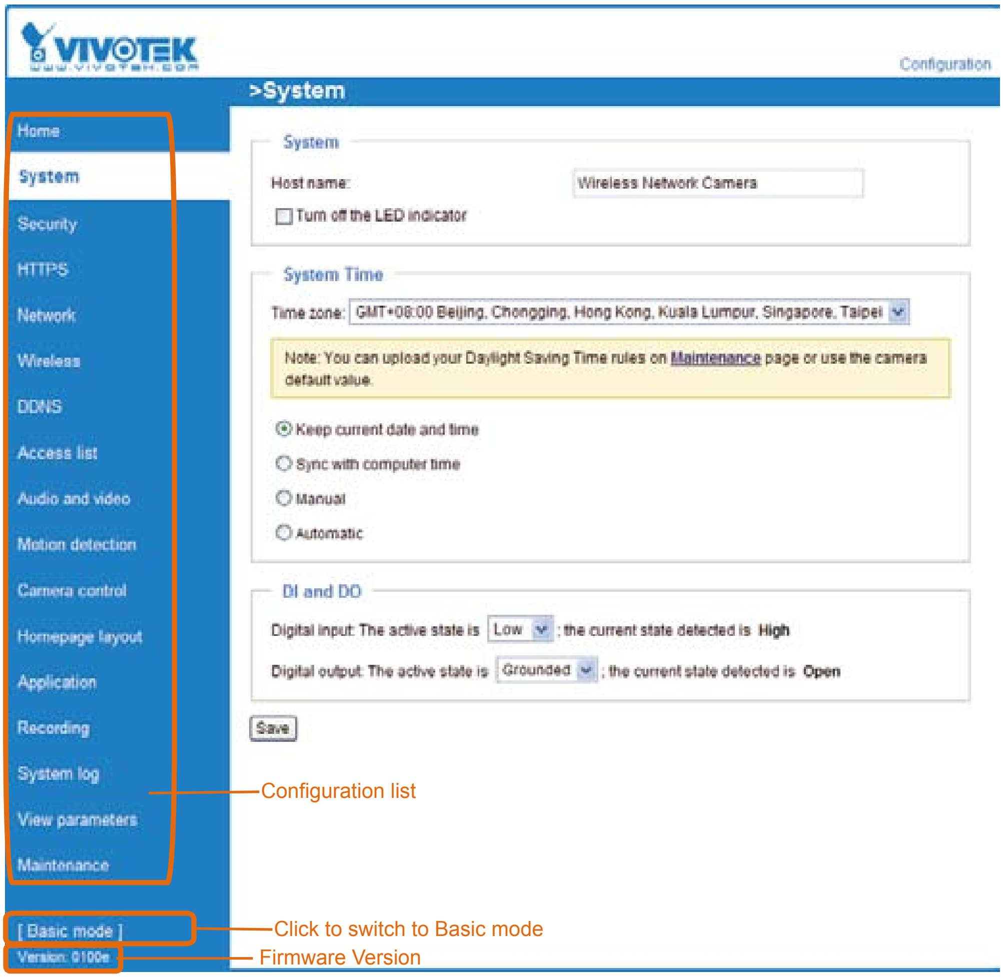
Version: 0100e

Configuration list

Click to switch to Advanced mode

Firmware Version

Advanced mode



>System

System

Host name: Wireless Network Camera

□ Turn off the LED indicator

System Time

Time zone: GMT+08:00 Beijing, Chongqing, Hong Kong, Kuala Lumpur, Singapore, Taipei

Note: You can upload your Daylight Saving Time rules on Maintenance page or use the camera default value.

● Keep current date and time
○ Sync with computer time
○ Manual
○ Automatic

DI and DO

Digital input: The active state is Low ; the current state detected is **High**

Digital output: The active state is Grounded ; the current state detected is **Open**

Save

Configuration list

Click to switch to Basic mode

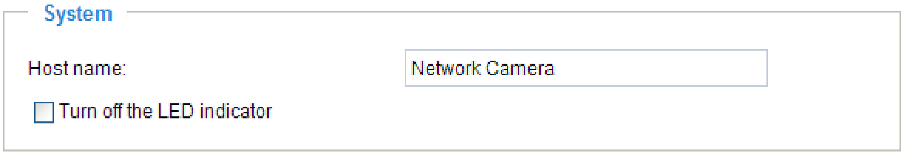
Firmware Version

Each function on the configuration list will be explained in the following sections. Those functions that only show in Advanced mode are marked with Advanced mode. If you want to set up advanced functions, please click **[Advanced mode]** on the bottom of the configuration list to quickly switch to Advanced mode.

System

This section explains how to configure the basic settings for the Network Camera, such as the host name and system time. It is composed of the following three columns: System, System Time and DI and DO. When completed with the settings on this page, click **Save** on the page bottom to take effect.

System



System

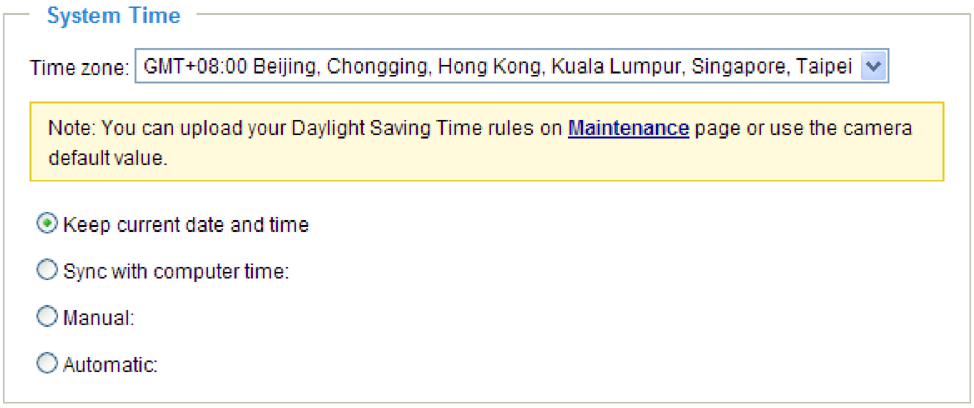
Host name: Network Camera

□ Turn off the LED indicator

Host name: Enter a desired name for the Network Camera. The text will be displayed at the top of the main page.

Turn off the LED indicators: If you don't want to let others know that the network camera is working, you can select this option to turn off the LED indicators.

System Time



System Time

Time zone: GMT+08:00 Beijing, Chongqing, Hong Kong, Kuala Lumpur, Singapore, Taipei

Note: You can upload your Daylight Saving Time rules on Maintenance page or use the camera default value.

● Keep current date and time

○ Sync with computer time:

○ Manual:

○ Automatic:

Keep current date and time: Select this option to reserve the current date and time of the Network Camera. The Network Camera's internal real-time clock maintains the date and time even when the power of the system is turned off.

Sync with computer time: Select this option to synchronize the date and time of the Network Camera with the local computer. The read-only date and time of the PC is displayed as updated.

Manual: The administrator can enter the date and time manually. Note that the date and time format are [yyyy/mm/dd] and [hh:mm:ss].

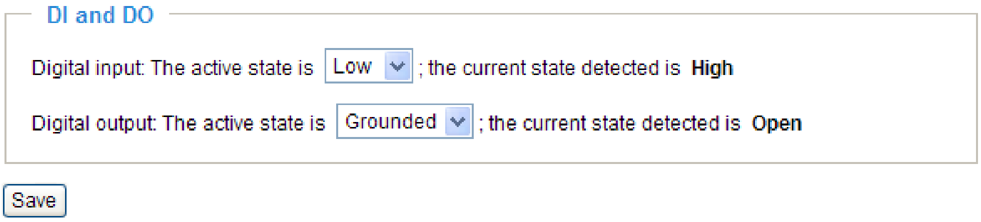
Automatic: The Network Time Protocol is a protocol serves synchronize computer clocks by periodically querying an NTP Server.

NTP server: Assign the IP address or domain name of the time-server. Leaving the text box blank connects the Network Camera to the default time-servers.

Update interval: Select to update the time with the NTP server on hourly, daily, weekly, or monthly basis.

Time zone Advanced mode: According to your local time zone, select one from the drop-down list. If you want to upload the daylight saving time rules on Maintenance page, please refer to Upload / Export Daylight Saving Time Configuration File on page 85 for details.

DI and DO



DI and DO

Digital input: The active state is Low ; the current state detected is **High**

Digital output: The active state is Grounded ; the current state detected is **Open**

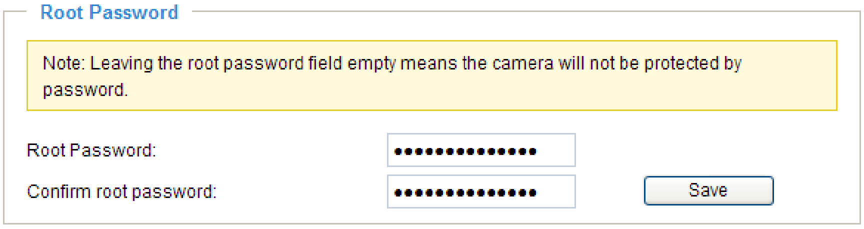
Digital input: Select High or Low to define normal status of the digital input. The Network Camera will report the current status.

Digital output: Select Grounded or Open to define normal status of the digital output. The Network Camera will show whether the trigger is activated or not.

Security

This section explains how to enable password protection and create multiple accounts.

Root Password



Root Password

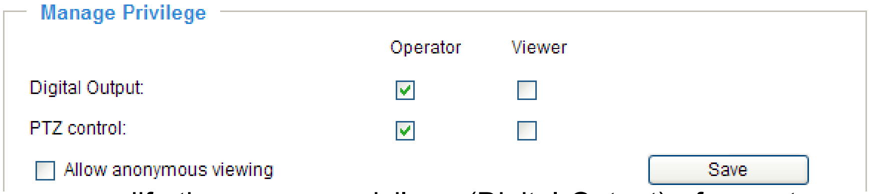
Note: Leaving the root password field empty means the camera will not be protected by password.

Root Password: ••••••••••••••

Confirm root password: ••••••••••••••

The administrator account name is “root”, which is permanent and can not be deleted. If you want to add more accounts in Manage User column, please apply a password for the “root” account first.
1. Type the password identically in both text boxes, and click **Save** to enable password protection.
2. A window will be prompted for authentication; type the correct user’s name and password in related fields to access the Network Camera.

Manage Privilege Advanced mode



Manage Privilege

	Operator	Viewer
Digital Output:	☑	□
PTZ control:	☑	□

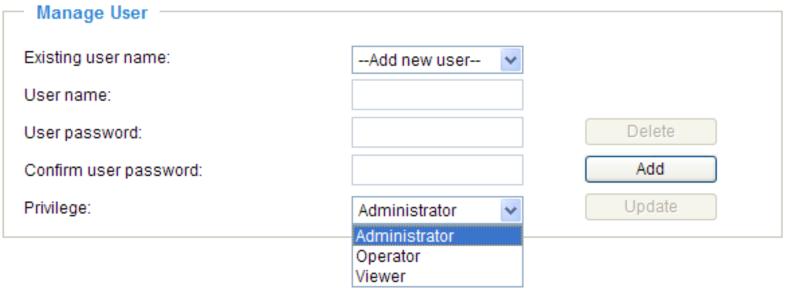
□ Allow anonymous viewing

Digital Output: You can modify the manage privilege (Digital Output) of operators or viewers. Check or uncheck the item, and then click **Save** to take effect. If you give Viewer the privilege to control Digital Output, Operator will also have the right to choose turn on or turn off the Digital Output devices on the main page. (Please refer to Main Page on page 18.)

PTZ control: You can modify the manage privilege (PTZ control) of operators or viewers.

Allow anonymous viewing: If you check this item, any clients can get access to the live streaming without entering User ID and Password.

Manage User



Manage User

Existing user name: --Add new user--

User name:

User password:

Confirm user password:

Privilege: Administrator

Administrators can add up to 20 user accounts.
1. Input the new user’s name and password.
2. Select the Privilege for new user account. Click **Add** to take effect.

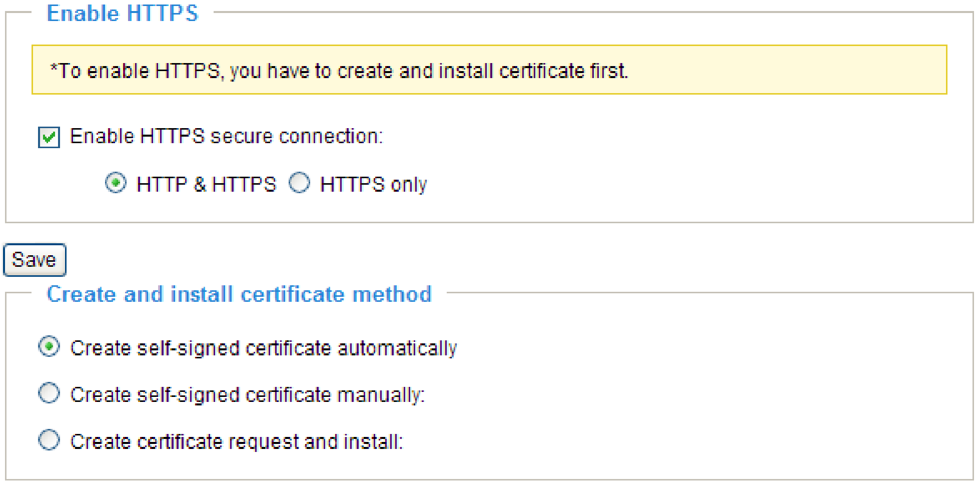
Access rights are sorted by user privilege (Administrator, Operator, and Viewer). Only administrators can access the Configuration page. Though operators can not access the Configuration page, they are capable of using the URL commands to get and set the value of parameters. For more information, please refer to URL Commands of the Network Camera on page 88. Viewers can only access the main page for live viewing.
Here you also can change user’s access rights or delete user accounts.
1. Select an existing account to modify.
2. Make necessary changes and then click **Update** or **Delete** to take effect.

HTTPS Advanced mode

This section explains how to enable authentication and encrypted communication over SSL. It helps protect streaming data transmission over the Internet.

Enable HTTPS

Check this item to enable HTTPS communication, and then select a connection option: "HTTP & HTTPS" or "HTTPS only". Note that you have to create and install certificate first in the second column before clicking the **Save** button.



Enable HTTPS

*To enable HTTPS, you have to create and install certificate first.

☑ Enable HTTPS secure connection:

● HTTP & HTTPS ○ HTTPS only

Create and install certificate method

● Create self-signed certificate automatically

○ Create self-signed certificate manually:

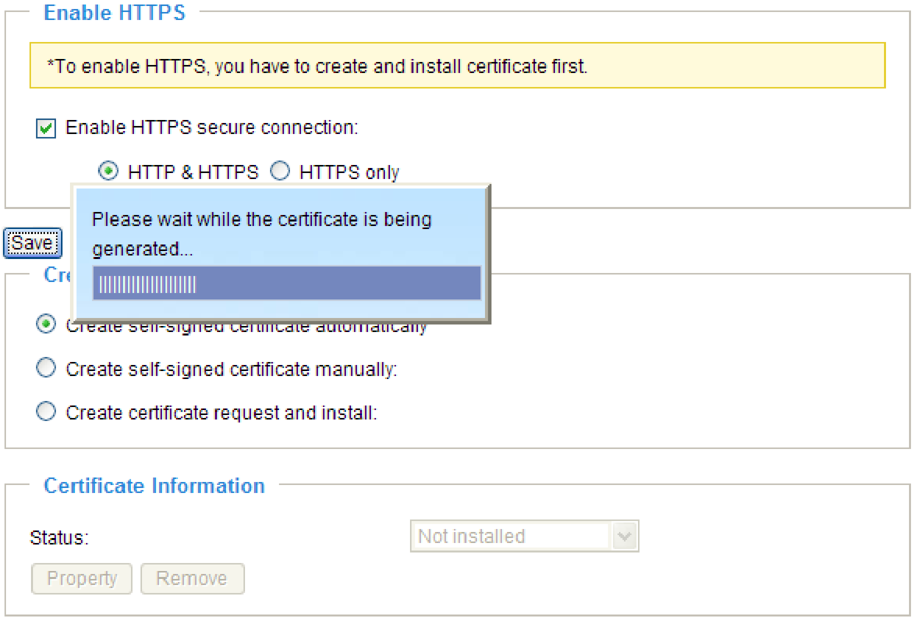
○ Create certificate request and install:

Create and Install Certificate Method

There are three ways to create and install certificate:

Create self-signed certificate automatically

1. Select this option.
2. In the first column, check **Enable HTTPS secure connection**, and then select a connection option: "HTTP & HTTPS" or "HTTPS only".
3. Click **Save** to generate certificate.



Enable HTTPS

*To enable HTTPS, you have to create and install certificate first.

☑ Enable HTTPS secure connection:

● HTTP & HTTPS ○ HTTPS only

Please wait while the certificate is being generated...

● Create self-signed certificate automatically

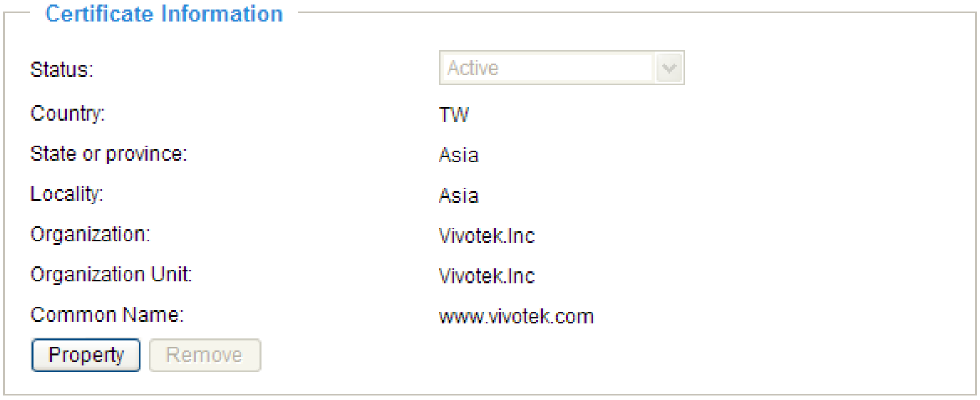
○ Create self-signed certificate manually:

○ Create certificate request and install:

Certificate Information

Status: Not installed

4. The Certificate Information will automatically show up in the third column as below. You can click **Property** to see the detailed information of the certificate.



Certificate Information

Status: Active

Country: TW

State or province: Asia

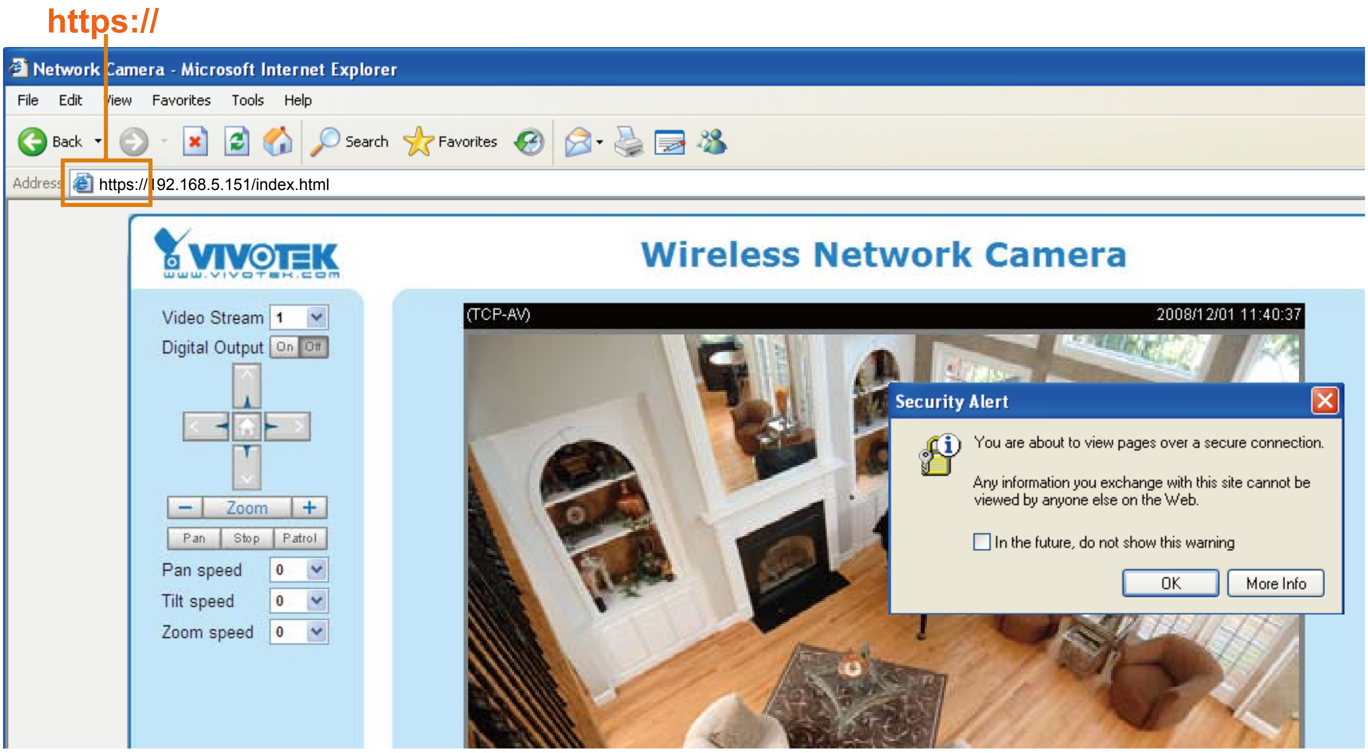
Locality: Asia

Organization: Vivotek.Inc

Organization Unit: Vivotek.Inc

Common Name: www.vivotek.com

5. Click **Home** to return to the main page. Change the address from "http://" to "https://" on the Address bar and press Enter on your keyboard. Some Security Alert dialogs will pop up. Click **OK** or **Yes** to enable HTTPS.



https://

Network Camera - Microsoft Internet Explorer

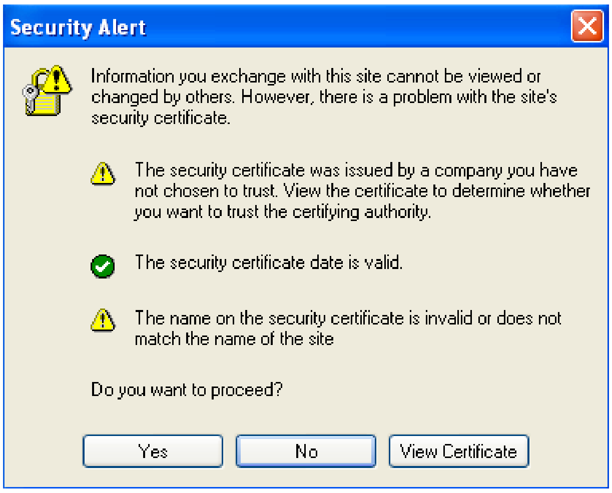
Address https://192.168.5.151/index.html

Security Alert

You are about to view pages over a secure connection.

Any information you exchange with this site cannot be viewed by anyone else on the Web.

□ In the future, do not show this warning



Security Alert

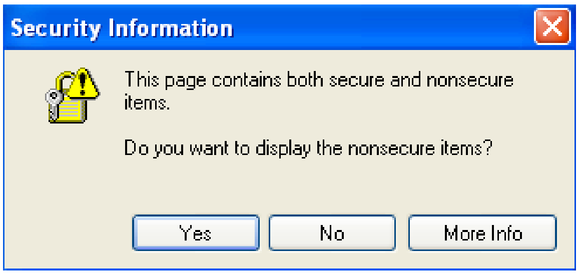
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

⚠ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?



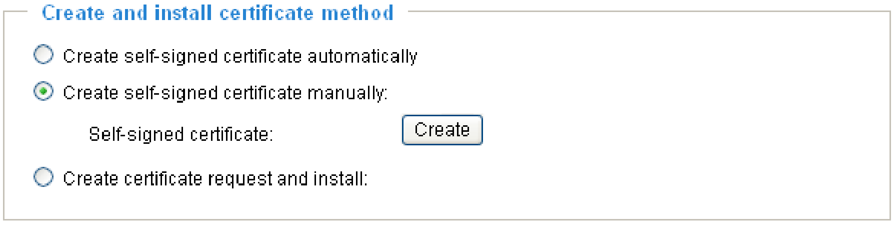
Security Information

This page contains both secure and nonsecure items.

Do you want to display the nonsecure items?

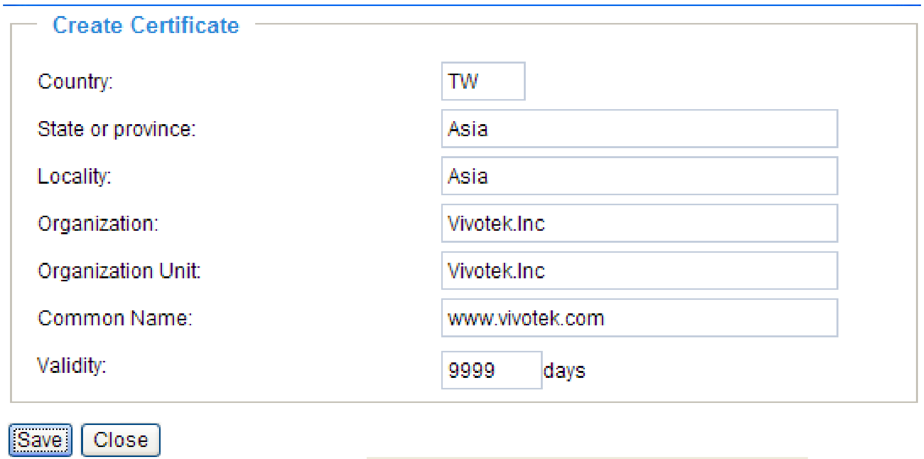
Create self-signed certificate manually

1. Select this option.
2. Click **Create** to open a Create Certificate page, and then click **Save** to generate the certificate.



Create and install certificate method

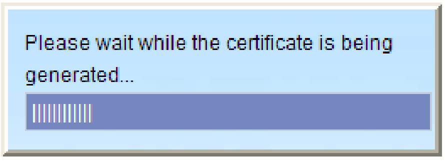
○ Create self-signed certificate automatically
● Create self-signed certificate manually:
Self-signed certificate: [Create]
○ Create certificate request and install:



Create Certificate

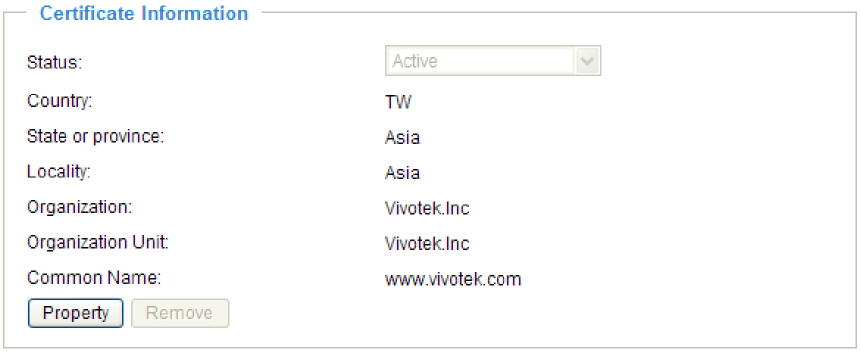
Country:	TW
State or province:	Asia
Locality:	Asia
Organization:	Vivotek.Inc
Organization Unit:	Vivotek.Inc
Common Name:	www.vivotek.com
Validity:	9999 days

[Save] [Close]



Please wait while the certificate is being generated...

3. The Certificate Information will automatically show up in the third column as below. You can click **Property** to see the detailed information of the certificate.



Certificate Information

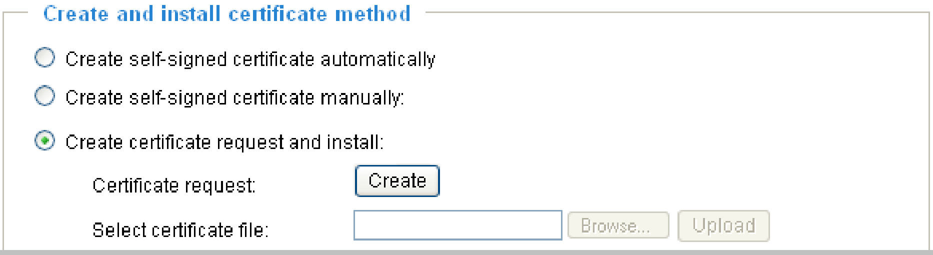
Status:	Active
Country:	TW
State or province:	Asia
Locality:	Asia
Organization:	Vivotek.Inc
Organization Unit:	Vivotek.Inc
Common Name:	www.vivotek.com

[Property] [Remove]

4. Please refer to step 5. on last page.

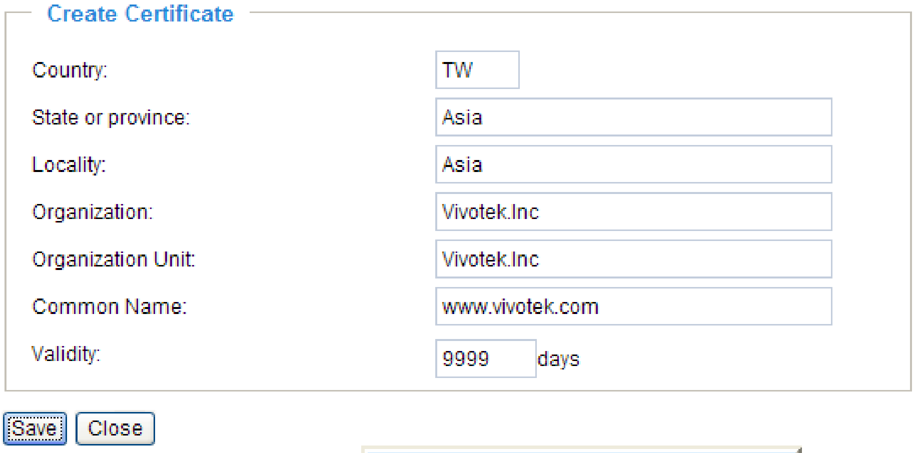
Create certificate and install : Select this option if you want to create a certificate from a certificate authority.

1. Select this option.
2. Click **Create** to open a Create Certificate page, and then click **Save** to generate the certificate.



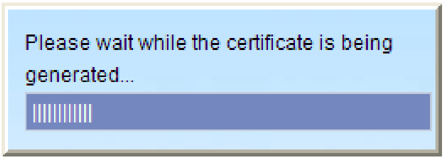
Create and install certificate method

○ Create self-signed certificate automatically
○ Create self-signed certificate manually:
● Create certificate request and install:
Certificate request: [Create]
Select certificate file: [Browse...] [Upload]



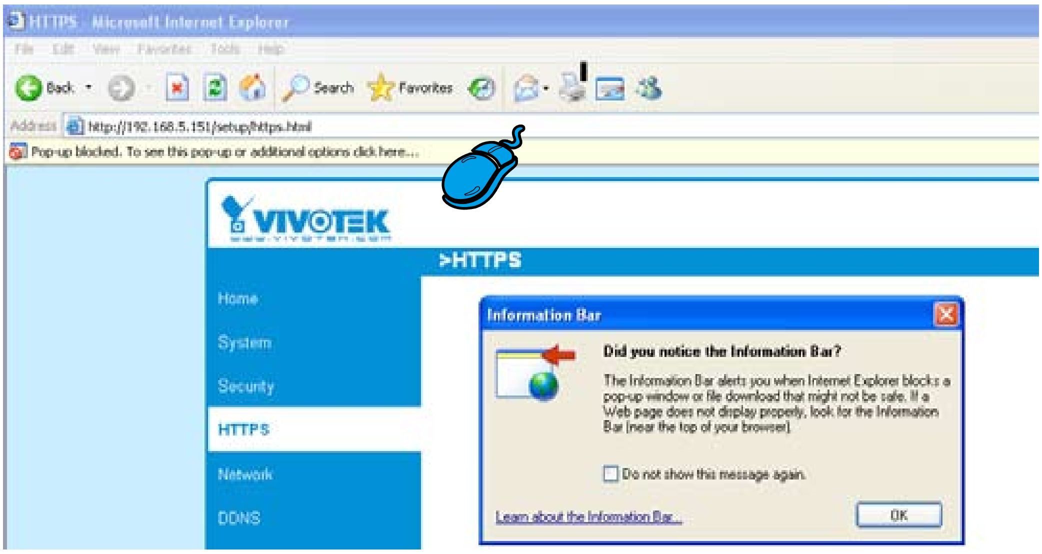
Create Certificate

Country:	TW
State or province:	Asia
Locality:	Asia
Organization:	Vivotek.Inc
Organization Unit:	Vivotek.Inc
Common Name:	www.vivotek.com
Validity:	9999 days



Please wait while the certificate is being generated...

3. If you see the following Information Bar, click **OK** and the menu bar on the top of the page to allow the Pop-ups.



HTTPS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://192.168.5.151/setup/https.html
VIVOTEK
>HTTPS
Home
System
Security
HTTPS
Network
DDNS
Information Bar
Learn about the Information Bar...
OK

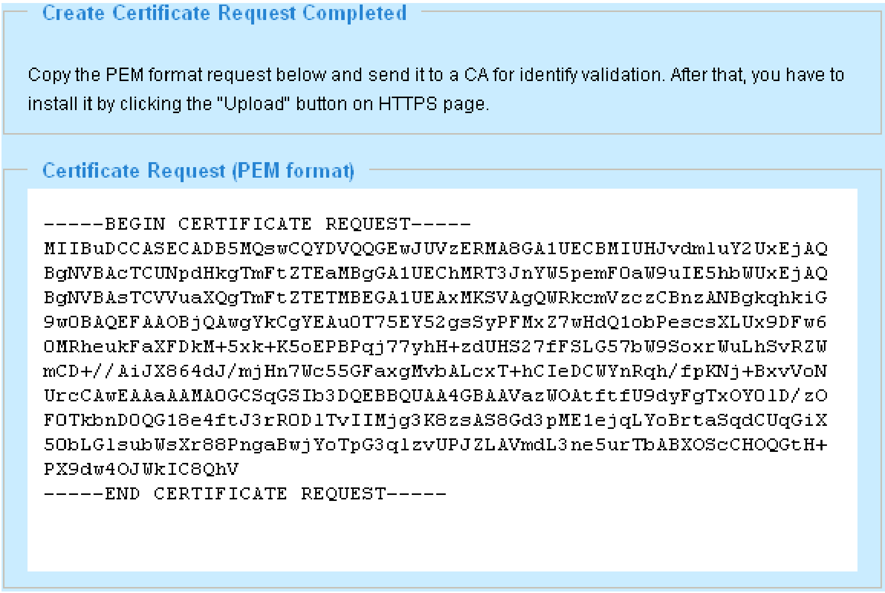
Pop-up blocked. To see this pop-up or additional options click here...

Did you notice the Information Bar?

The Information Bar alerts you when Internet Explorer blocks a pop-up window or file download that might not be safe. If a Web page does not display properly, look for the Information Bar (near the top of your browser).

□ Do not show this message again.

4. The Pop-up window shows an example of a certificate request.



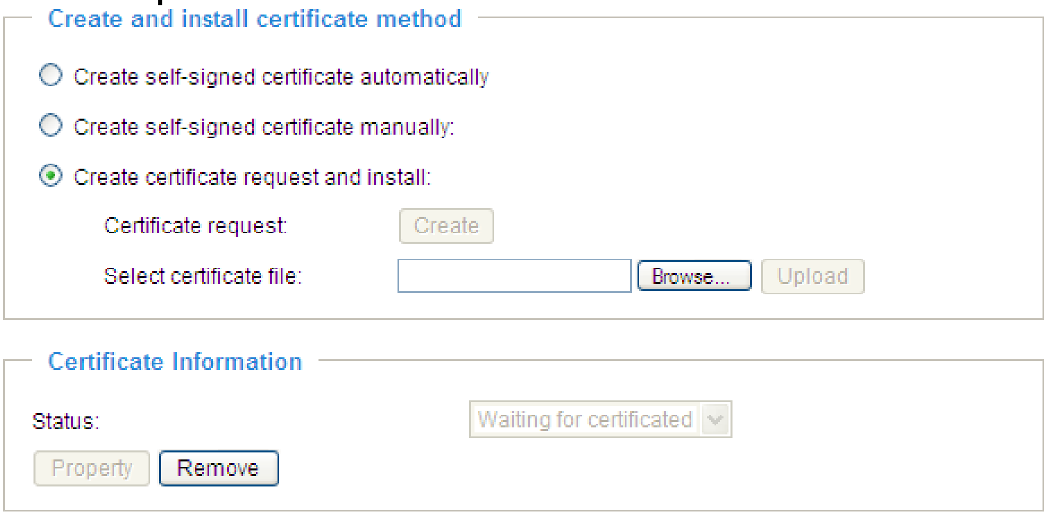
Create Certificate Request Completed

Copy the PEM format request below and send it to a CA for identify validation. After that, you have to install it by clicking the "Upload" button on HTTPS page.

Certificate Request (PEM format)

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBuDCCASECADB5MQswCQYDVQQGEwJUVzERMA8GA1UECBMIUHJvdmluY2UxEjAQ
BgNVBAcTCUNpdHkgTmFtZTEaMBgGA1UEChMRT3JnYW5pemF0aW9uIE5hbWUxEjAQ
BgNVBAsTCVVuaXQgTmFtZTETMBEGA1UEAxMKSVAgQWRkcmVzczCBnzANBgkqhkiG
9w0BAQEFAAOBjQAwgYkCgYEAu0T75EY52gsSyPFMxZ7wHdQ1obPescsXLUx9DFw6
OMRheukFaXFDkM+5xk+K5oEPBPqj77yhH+zdUHS27fFSLG57bW9SoxrWuLhSvRZW
mCD+//AiJX864dJ/mjHn7Wc55GFaxgMvbALcxT+hCIeDCWYnRqh/fpKNj+BxvVoN
UrcCAwEAAaAAMA0GCSqGSIb3DQEBBQUAA4GBAAVazWOAtftfU9dyFgTxOYO1D/zO
FOTkbnDOQG18e4ftJ3rROD1TvIIMjg3K8zsAS8Gd3pME1ejqLYoBrtaSqdCUqGiX
5ObLG1subWsXr88PngaBwjYoTpG3q1zvUPJZLAVmdL3ne5urTbABXOScCHOQGtH+
PX9dw4OJWkIC8QhV
-----END CERTIFICATE REQUEST-----
```

5. Look for a trusted certificate authority that issues digital certificates. Enroll the Network Camera. Wait for the certificate authority to issue a SSL certificate; click **Browse...** to search for the issued certificate, then click **Upload** in the second column.



Create and install certificate method

○ Create self-signed certificate automatically

○ Create self-signed certificate manually:

● Create certificate request and install:

Certificate request:

Select certificate file:

Certificate Information

Status: Waiting for certificated

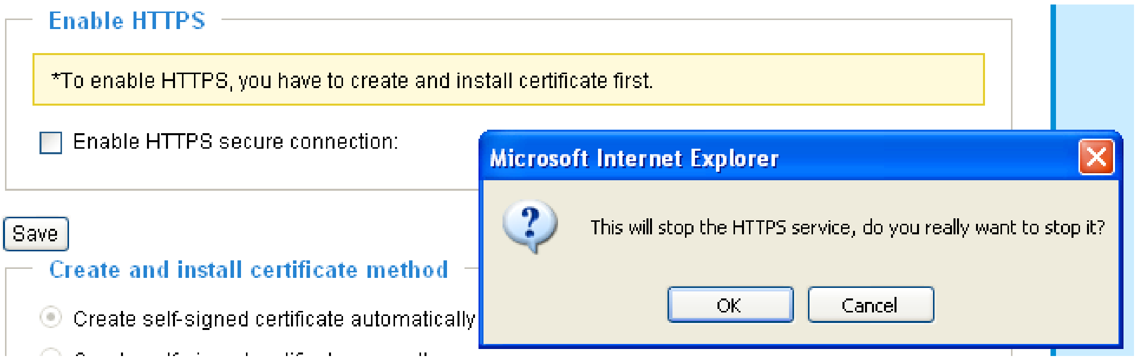
6. Please refer to step 4. and 5. on page 29.

NOTE

► *How to cancel HTTPS settings?*

*1. Uncheck **Enable HTTPS secure connection** in the first column and then click **Save**, then a warning dialog will pop up.*

*2. Click **OK** to disable HTTPS.*



Enable HTTPS

*To enable HTTPS, you have to create and install certificate first.

□ Enable HTTPS secure connection:

Create and install certificate method

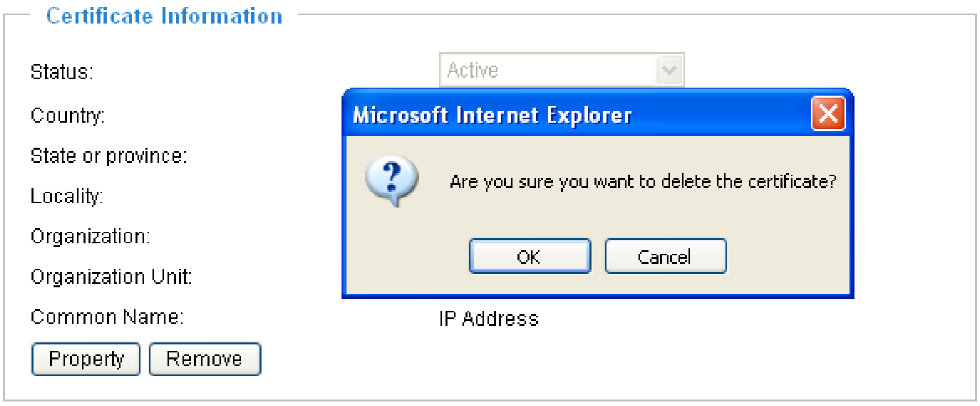
● Create self-signed certificate automatically

Microsoft Internet Explorer

This will stop the HTTPS service, do you really want to stop it?

3. The webpage will redirect to non-https page automatically.

► *If you want to create and install other certificate, please remove the existing one. To remove the signed certificated, uncheck the **Enable HTTPS secure connection** in the first column and click **Save**. Then click **Remove** to erase the certificate.*



Certificate Information

Status: Active

Country:

State or province:

Locality:

Organization:

Organization Unit:

Common Name: IP Address

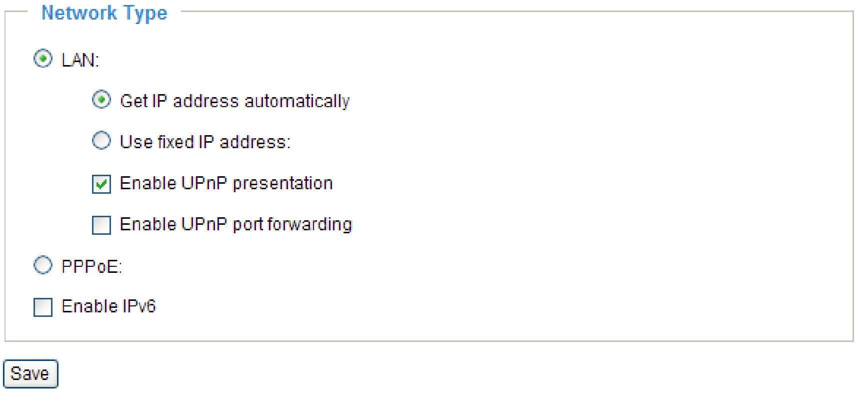
Microsoft Internet Explorer

Are you sure you want to delete the certificate?

Network

This section explains how to configure wired network connection for the Network Camera.

Network Type



Network Type

● LAN:

● Get IP address automatically

○ Use fixed IP address:

☑ Enable UPnP presentation

□ Enable UPnP port forwarding

○ PPPoE:

□ Enable IPv6

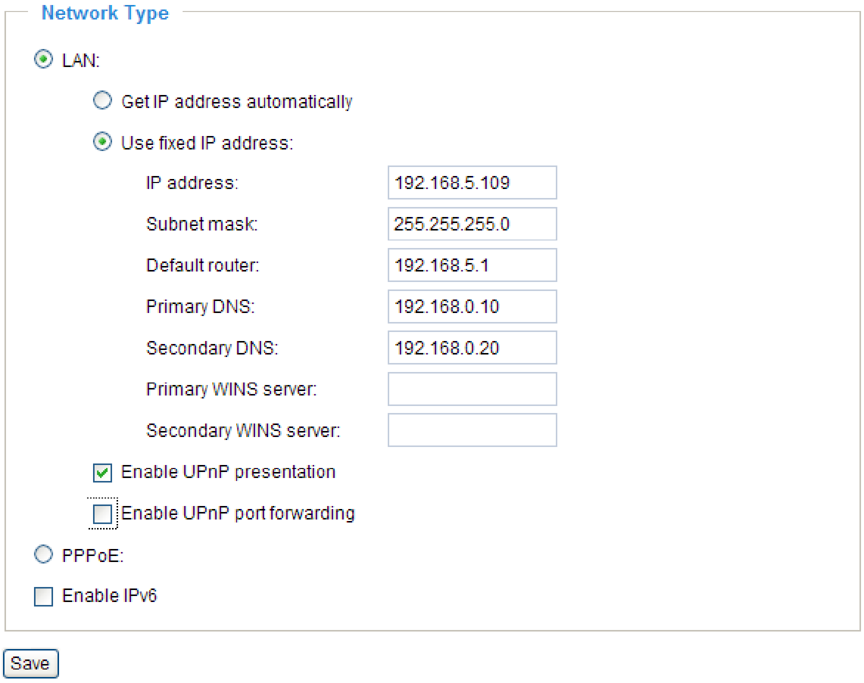
Save

LAN

Select this option when the Network Camera is deployed in a local area network (LAN) and is intended to be accessed by local computers. The default setting of Network Type is LAN. Remember to click **Save** when you complete the Network setting.

Get IP address automatically: Select this option to obtain an available dynamic IP address assigned by a DHCP server each time the camera is connected to the LAN.

Use fixed IP address: Select this option to manually assign a static IP address to the Network Camera.



Network Type

● LAN:

○ Get IP address automatically

● Use fixed IP address:

IP address:	192.168.5.109
Subnet mask:	255.255.255.0
Default router:	192.168.5.1
Primary DNS:	192.168.0.10
Secondary DNS:	192.168.0.20
Primary WINS server:	
Secondary WINS server:	

☑ Enable UPnP presentation

□ Enable UPnP port forwarding

○ PPPoE:

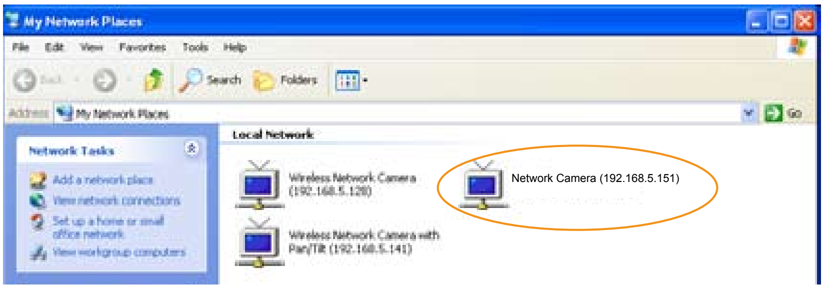
□ Enable IPv6

Save

1. You can make use of VIVOTEK installation wizard II on the software CD to easily set up the Network Camera in LAN. Please refer to Software installation on page 12 for details.
2. Enter the static IP, Subnet mask, Default router, Primary DNS provided by your ISP.

Enable UPnP presentation: Select this option to enable UPnP™ presentation for your Network Camera so that whenever a Network Camera is presented to the LAN, shortcuts of connected Network Cameras will be listed in My Network Places. You can click the shortcut to link to the web browser. Currently, UPnP™ is supported by Windows XP or later. Note that to utilize this feature, please make sure the

UPnP^{TM} component is installed on your computer.


My Network Places
File Edit View Favorites Tools Help
Back Search Folders
Address My Network Places Go
Network Tasks
Add a network place
View network connections
Set up a home or small office network
View workgroup computers
Local Network
Wireless Network Camera (192.168.5.128)
Network Camera (192.168.5.151)
Wireless Network Camera with Pan/Tilt (192.168.5.141)

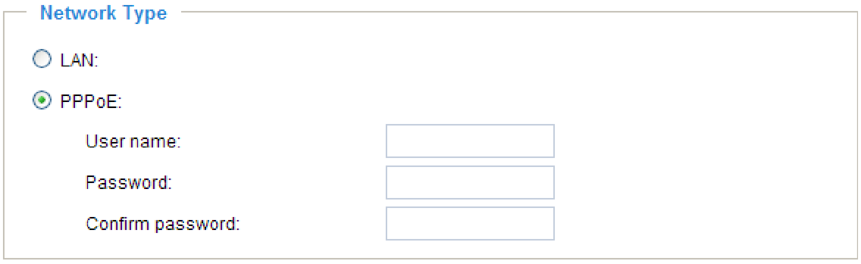
Enable UPnP port forwarding: To access the Network Camera from the Internet, select this option to allow the Network Camera to open ports on the router automatically so that video streams can be sent out from a LAN. To utilize of this feature, make sure that your router supports UPnP^{TM} and it is activated.

PPPoE (Point-to-point over Ethernet)

Select this option to configure your Network Camera to make it accessible from anywhere as long as there is an Internet connection. Note that to utilize this feature, it requires an account provided by your ISP.

Follow the steps below to acquire your Network Camera's public IP address.

1. Set up the Network Camera in LAN.
2. Go to Home > Configuration > Application > Server Settings (please refer to Server Settings on page 72) to add a new server -- email or FTP server.
3. Go to Configuration > Application > Media Settings (please refer to Media Settings on page 75). Select System log so that you will receive a list of system log in TXT file format which contains the Network Camera's public IP address in your email or on the FTP server.
4. Go to Configuration > Network > Network Type. Select PPPoE and enter the user name and password provided by your ISP. Click **Save** to take effect.



Network Type

○ LAN:

● PPPoE:

User name:

Password:

Confirm password:

5. The Network Camera starts to reboot.
6. Disconnect the power source of the Network Camera; remove it from the LAN environment to the Internet.

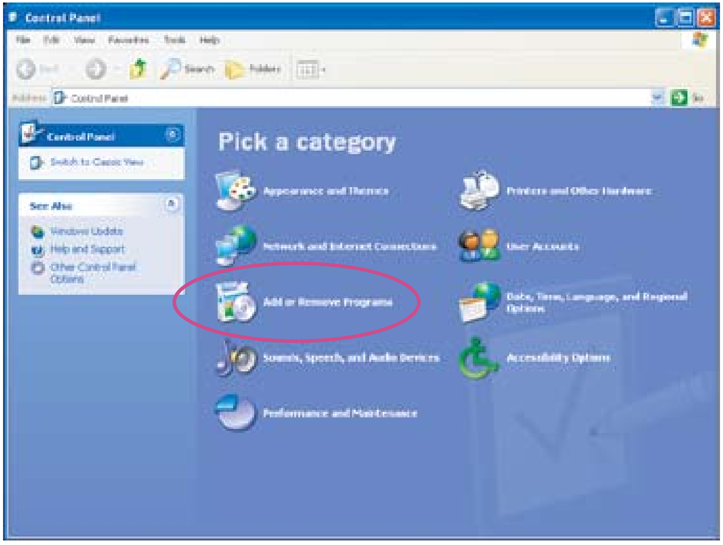
NOTE

► *If the default ports are already used by other device connecting to the same router, the Network Camera will select other ports for the Network Camera.*

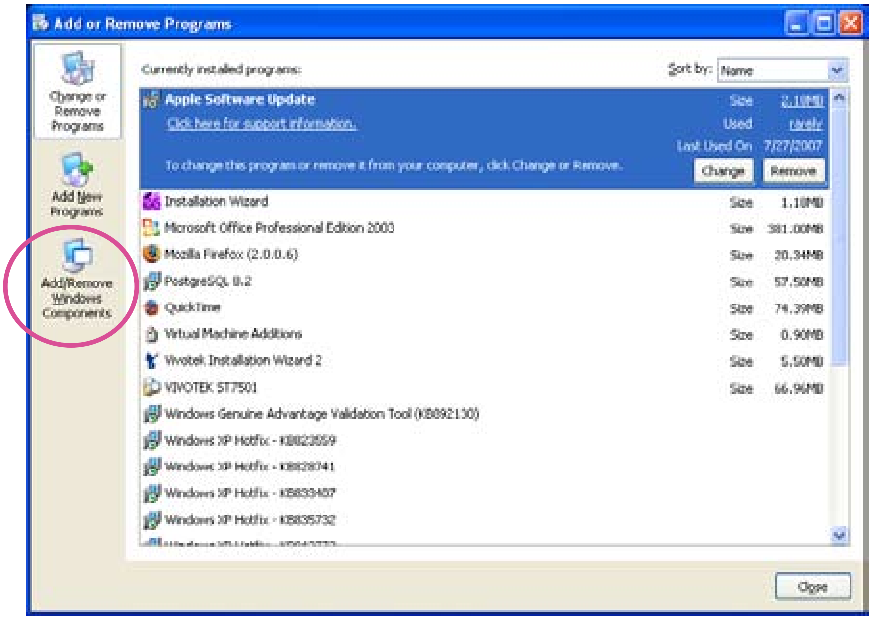
► *If UPnP^{TM} is not supported by your router, you will see the following message:*
Error: Router does not support UPnP port forwarding.

► *Steps to enable UPnP^{TM} user interface on your computer:*
Note that you must log on to the computer as a system administrator to install the UPnP^{TM} components.

*1. Go to Start, click **Control Panel**, and then click **Add or Remove Programs**.*


Control Panel
File Edit View Favorites Tools Help
Back Search Folders
Address Control Panel Go
Control Panel
Switch to Classic View
See Also
Windows Update
Help and Support
Other Control Panel Options
Pick a category
Appearance and Themes
Printers and Other Hardware
Network and Internet Connections
User Accounts
Add or Remove Programs
Date, Time, Language, and Regional Options
Sounds, Speech, and Audio Devices
Accessibility Options
Performance and Maintenance

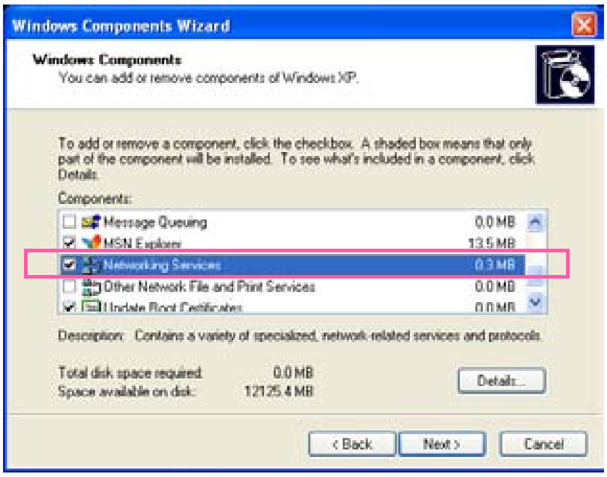
*2. In the Add or Remove Programs dialog box, click **Add/Remove Windows Components**.*



Currently installed programs:

Apple Software Update Click here for support information. To change this program or remove it from your computer, click Change or Remove.	Size Used Last Used On	2.10MB rarely 7/27/2007
Installation Wizard	Size	1.10MB
Microsoft Office Professional Edition 2003	Size	381.00MB
Mozilla Firefox (2.0.0.6)	Size	20.34MB
PostgreSQL 8.2	Size	57.50MB
QuickTime	Size	74.39MB
Virtual Machine Additions	Size	0.90MB
Vivotek Installation Wizard 2	Size	5.50MB
VIVOTEK ST7501	Size	66.96MB
Windows Genuine Advantage Validation Tool (KB892130)		
Windows XP Hotfix - KB823559		
Windows XP Hotfix - KB828741		
Windows XP Hotfix - KB833407		
Windows XP Hotfix - KB835732		

*3. In the Windows Components Wizard dialog box, select **Networking Services** and then click **Details**.*



Windows Components

You can add or remove components of Windows XP.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

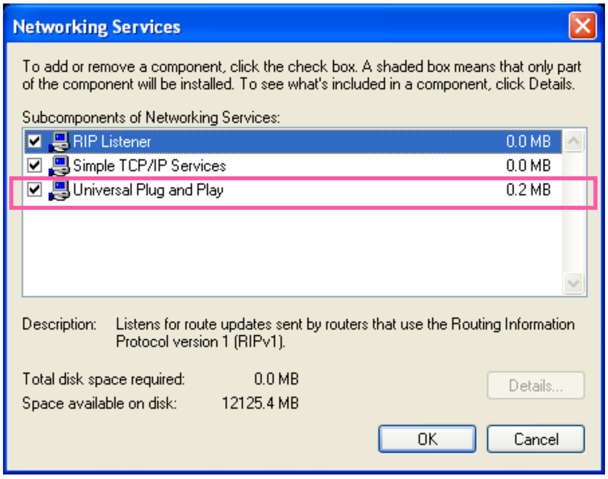
☐	Message Queuing	0.0 MB
☑	MSN Explorer	13.5 MB
☑	Networking Services	0.3 MB
☐	Other Network File and Print Services	0.0 MB
☑	Update Root Certificates	0.0 MB

Description: Contains a variety of specialized, network-related services and protocols.

Total disk space required: 0.0 MB

Space available on disk: 12125.4 MB

*4. In the Networking Services dialog box, select **Universal Plug and Play** and then click **OK**.*



To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Networking Services:

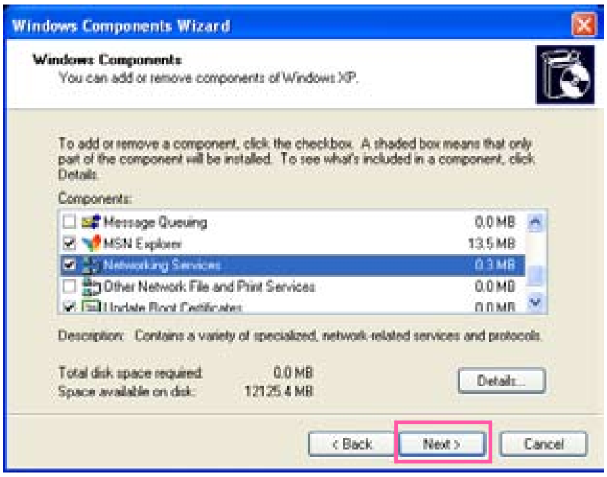
☑ RIP Listener	0.0 MB
☑ Simple TCP/IP Services	0.0 MB
☑ Universal Plug and Play	0.2 MB

Description: Listens for route updates sent by routers that use the Routing Information Protocol version 1 (RIPv1).

Total disk space required: 0.0 MB

Space available on disk: 12125.4 MB

*5. Click **Next** in the following window.*



You can add or remove components of Windows XP.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

☐ Message Queuing	0.0 MB
☑ MSN Explorer	13.5 MB
☑ Networking Services	0.3 MB
☐ Other Network File and Print Services	0.0 MB
☑ Update Root Certificates	0.0 MB

Description: Contains a variety of specialized, network-related services and protocols.

Total disk space required: 0.0 MB

Space available on disk: 12125.4 MB

*6. Click **Finish**. UPnP™ is enabled.*

► *How does UPnP™ work?*
UPnP™ networking technology provides automatic IP configuration and dynamic discovery of devices added to a network. Services and capabilities offered by networked devices, such as printing and file sharing, are available among each other without bothersome network configuration. In the case of Network Cameras, you will see Network Camera shortcuts at My Network Places.

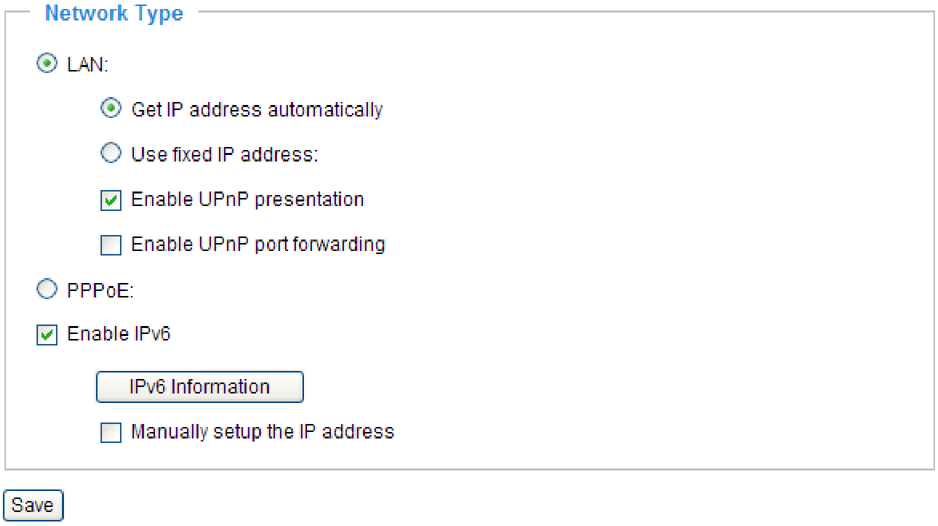
► *Enabling UPnP port forwarding allows the Network Camera to open secondary HTTP port on the router, not HTTP port, meaning that you have to add the secondary HTTP port number behind the Network Camera's public address in order to access the Network Camera from the Internet. For example, when the HTTP port is set to 80 and the secondary HTTP port is set to 8080, refer to the list below for the Network Camera's IP address.*

From the Internet	In LAN
http://203.67.124.123:8080	http://192.168.4.160 or http://192.168.4.160:8080

► *If the PPPoE settings are incorrectly configured or the Internet access is not working, restore the Network Camera to factory default; please refer to Restore on page 84 for details. After the Network Camera is reset to factory default, it is accessible in LAN.*

Enable IPv6

Select this option and then click **Save** to enable IPv6 settings.
Please note that it only works if your network environment and hardware equipment support IPv6. As for the web browse, you have to update to Microsoft® Internet Explorer 6.5, Mozilla Firefox 3.0 or above.



Network Type

● LAN:

● Get IP address automatically

○ Use fixed IP address:

☑ Enable UPnP presentation

□ Enable UPnP port forwarding

○ PPPoE:

☑ Enable IPv6

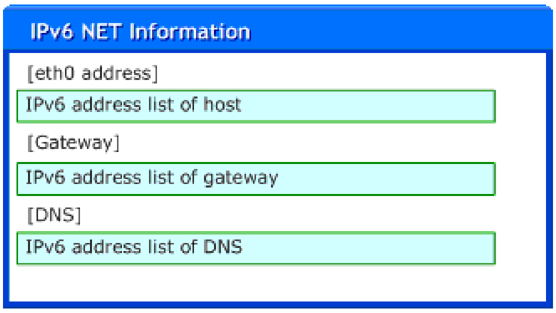
IPv6 Information

□ Manually setup the IP address

Save

When IPv6 is enabled, by default, the network camera will listen to router advertisements and be assigned with a link-local IPv6 address accordingly.

IPv6 Information: Click this button to get the IPv6 information as below.



IPv6 NET Information

[eth0 address]

IPv6 address list of host

[Gateway]

IPv6 address list of gateway

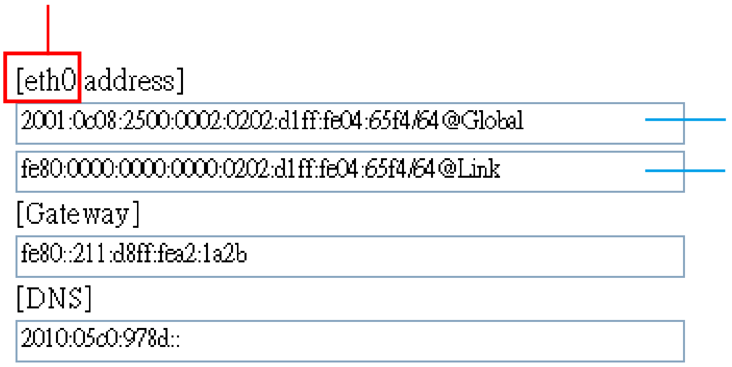
[DNS]

IPv6 address list of DNS

If your IPv6 settings are successful, the IPv6 addresses list will listed in the pop-up window. The IPv6 address will be in

For example:

refer to Ethernet



[eth0 address]

2001:0c08:2500:0002:0202:d1ff:fe04:65f4/64@Global

fe80:0000:0000:0000:0202:d1ff:fe04:65f4/64@Link

[Gateway]

fe80::211:d8ff:fea2:1a2b

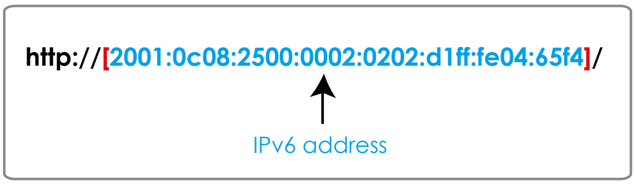
[DNS]

2010:05c0:978d::

Link-global IPv6 address/network mask

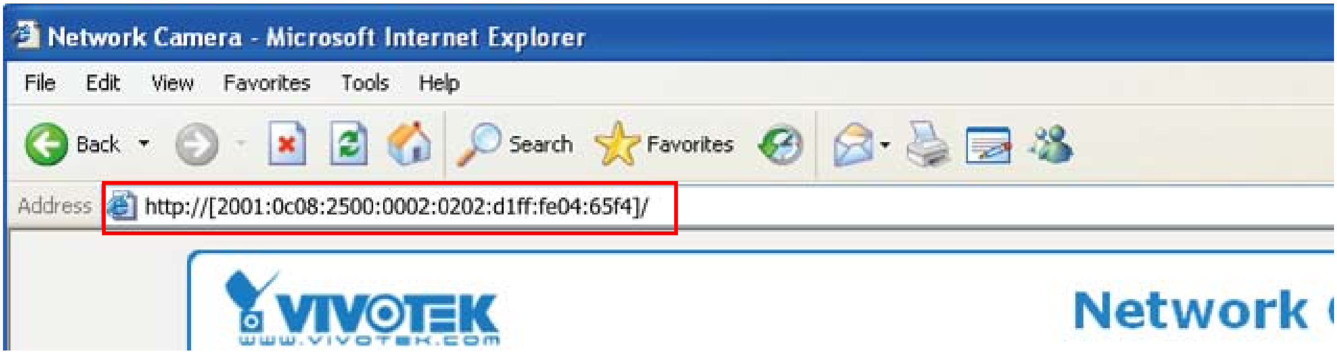
Link-local IPv6 address/network mask

Please follow the steps below to link to IPv6 address:
1. Open your web browser.
2. Enter the link-global or link-local IPv6 address to the address bar of your web browser.
3. The format should be:



http://[2001:0c08:2500:0002:0202:d1ff:fe04:65f4]/

4. Press **Enter** on the keyboard or click **Refresh** button to refresh the webpage.
   For example:

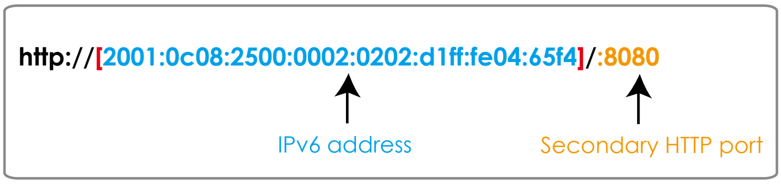


Network Camera - Microsoft Internet Explorer

Address http://[2001:0c08:2500:0002:0202:d1ff:fe04:65f4]/

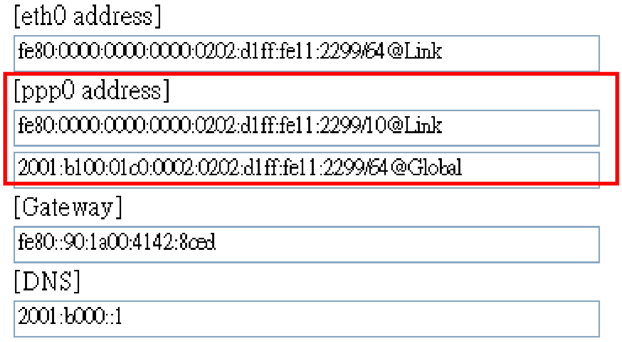
NOTE

► *If you have the Secondary HTTP port (the default value is 8080), you can also link to the webpage in the following address format: (Please refer to **HTTP** on page 39 for detailed information.)*



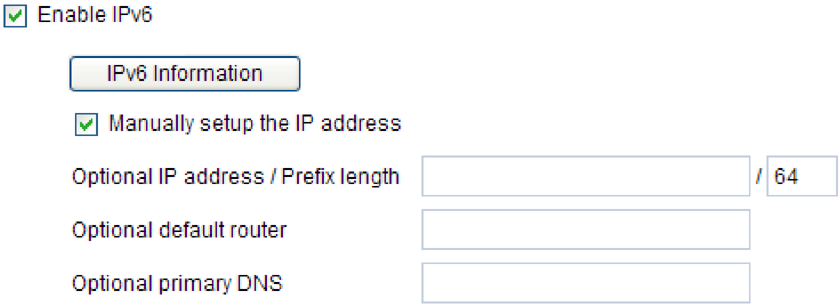
http://[2001:0c08:2500:0002:0202:d1ff:fe04:65f4]/:8080

► *If you choose PPPoE as the Network Type, the [PPP0 address] will show up in the IPv6 information column as below.*



[eth0 address]
fe80:0000:0000:0000:0202:d1ff:fe11:2299/64@Link
[ppp0 address]
fe80:0000:0000:0000:0202:d1ff:fe11:2299/10@Link
2001:b100:01c0:0002:0202:d1ff:fe11:2299/64@Global
[Gateway]
fe80::90:1a00:4142:8ced
[DNS]
2001:b000::1

Manually setup the IP address: Select this option to manually setup IPv6 settings if your network environment does not have DHCPv6 server and router advertisements enabled routers.
If you check this item, the following blanks will be displayed for you to enter corresponding information:



☑ Enable IPv6

☑ Manually setup the IP address

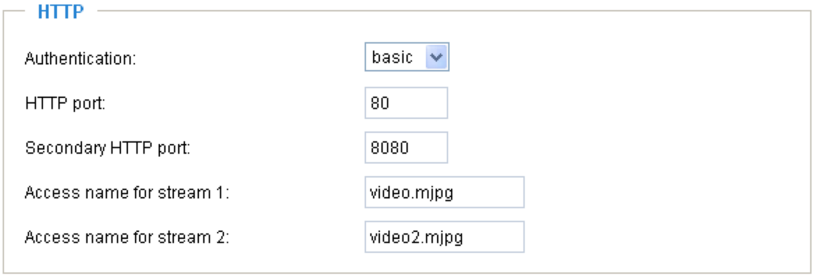
Optional IP address / Prefix length ______ / 64

Optional default router ______

Optional primary DNS ______

HTTP Advanced mode

To utilize the HTTP authentication, make sure that your have set a password for the Network Camera first; please refer to Security on page 27 for details.



HTTP

Authentication: basic

HTTP port: 80

Secondary HTTP port: 8080

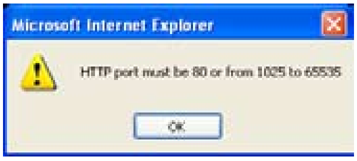
Access name for stream 1: video.mjpg

Access name for stream 2: video2.mjpg

Authentication: Depending on your network security requirements, the Network Camera provides two types of security settings for a HTTP transaction: basic and digest.

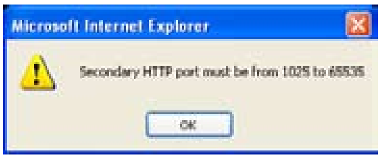
If **basic** authentication is selected, the password is sent in plain text format; there can be potential risks of being intercepted. If **digest** authentication is selected, user credentials are encrypted in MD5 algorithm and thus provide better protection against unauthorized accesses.

HTTP port / Secondary HTTP port: By default, the HTTP port is set to 80 and the secondary HTTP port is set to 8080. Also, they can be assigned with another port number between 1025 and 65535. If the ports are incorrectly assigned, the following warning messages will be displayed:



Microsoft Internet Explorer

HTTP port must be 80 or from 1025 to 65535



Microsoft Internet Explorer

Secondary HTTP port must be from 1025 to 65535

To access the Network Camera in LAN, both HTTP port and secondary HTTP port can be used to access the Network Camera. For example, when the HTTP port is set to 80 and the secondary HTTP port is set to 8080, refer to the list below for the Network Camera's IP address.

In LAN
http://192.168.4.160 or http://192.168.4.160:8080

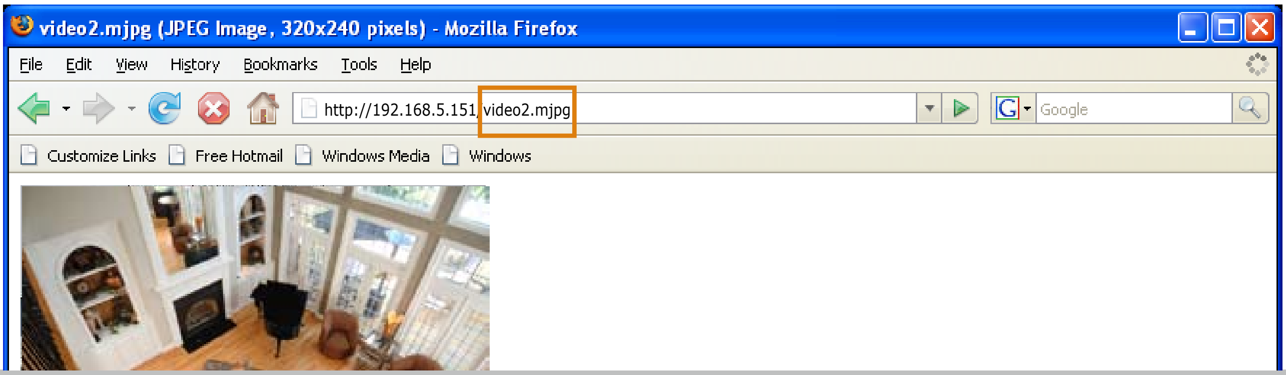
Access name for stream 1 / Access name for stream 2: The access name is used to differentiate the streaming source.

When using Mozilla Firefox or Netscape to access the Network Camera, and the video mode is set to JPEG, users will receive continuous JPEG pictures. This technology, known as "server push", allows the Network Camera to feed live pictures to Mozilla Firefox and Netscape.

URL command -- http://<ip address>:<http port>/<access name for stream1 or stream2>

For example, when the Access name for stream 2 is set to video2.mjpg:

1. Launch Mozilla Firefox or Netscape.
2. Type the URL command in the address bar. Press **Enter**.
3. The JPEG images will be displayed in your web browser.



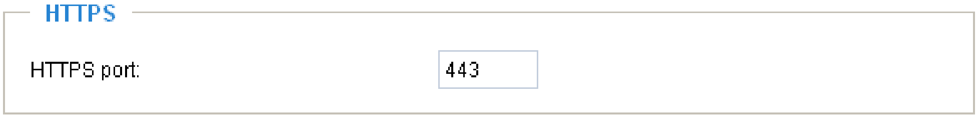
video2.mjpg (JPEG Image, 320x240 pixels) - Mozilla Firefox

http://192.168.5.151/video2.mjpg

NOTE

► *Microsoft® Internet Explorer does not support server push technology; therefore, using http://<ip address>:<http port>/<access name for stream1 or stream2> will fail to access the Network Camera.*

HTTPS

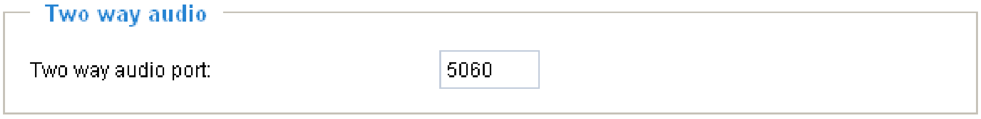


HTTPS

HTTPS port: 443

By default, the HTTPS port is set to 443. It also can be assigned with another port number between 1025 and 65535.

Two way audio



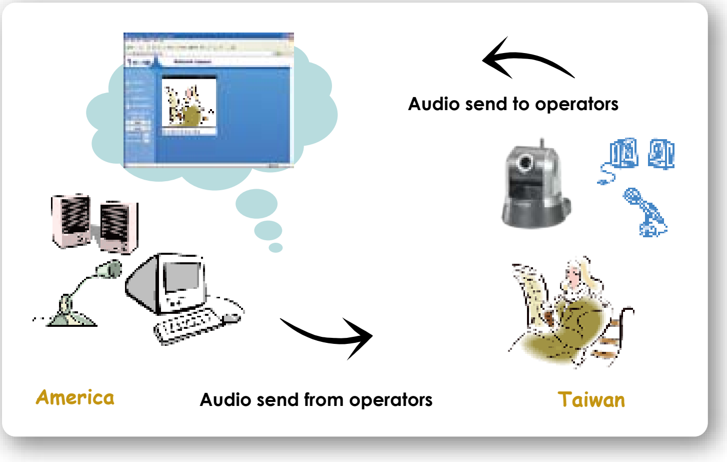
Two way audio

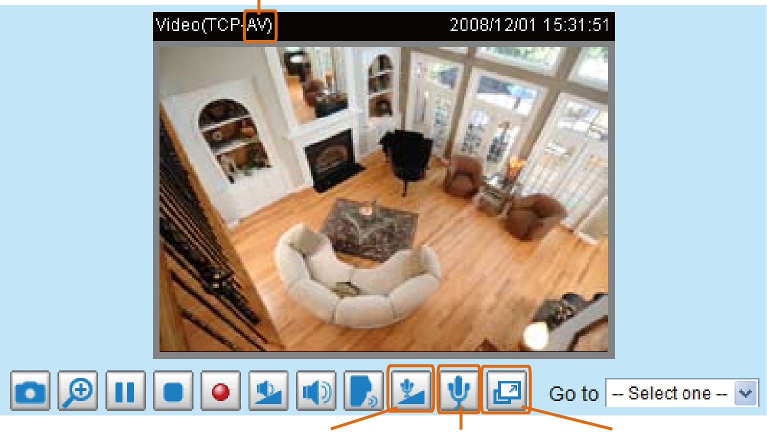
Two way audio port: 5060

By default, the two way audio port is set to 5060. Also, it can be assigned with another port number between 1025 and 65535.

The Network Camera supports two way audio communication so that operators can transmit and receive audio simultaneously. By using the Network Camera's built-in or external microphone and an external speaker, you can communicate with people around the Network Camera.

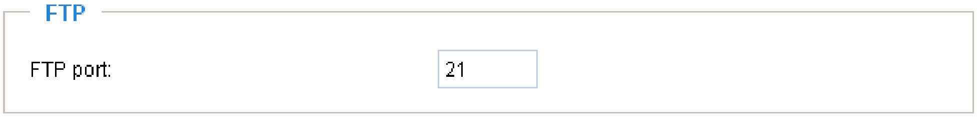
Note that as JPEG only transmits a series of JPEG images to the client, to enable two-way audio function, make sure the video mode is set to "MPEG-4" on Audio and Video settings page and the media option is set to "Video and Audio" on the Client Settings page. Please refer to Client Settings on page 22 and Audio and Video Settings on page 52.





Click to enable audio transmission to the Network Camera; click to adjust the volume of microphone; click to turn off the audio. To stop talking, click again.

FTP



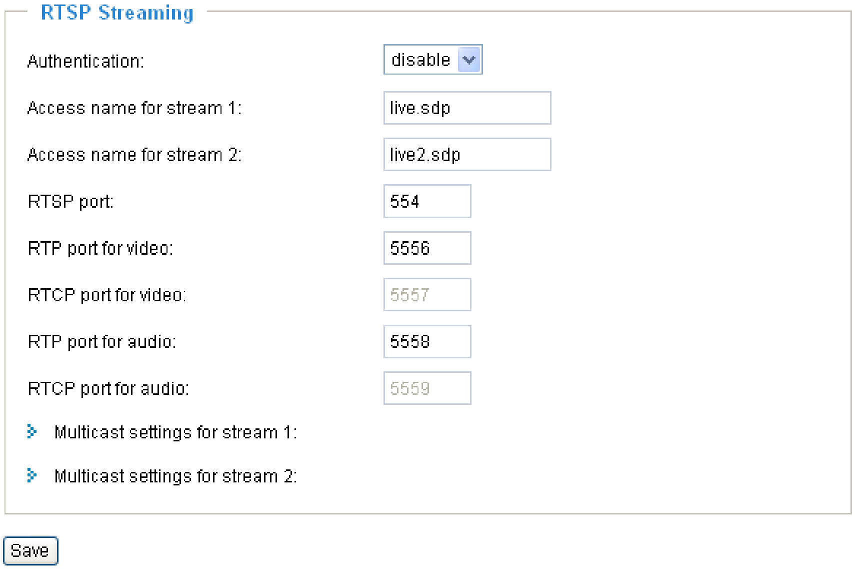
FTP

FTP port: 21

FTP server allows the user to save recorded video clips. And you can utilize VIVOTEK Installation Wizard 2 to upgrade firmware via FTP server. By default, the FTP port is set to 21. It also can be assigned with another port number between 1025 and 65535.

RTSP Streaming

To utilize the RTSP streaming authentication, make sure that your have set a password for the Network Camera first; please refer to Security on page 27 for details.



RTSP Streaming

Authentication:	disable
Access name for stream 1:	live.sdp
Access name for stream 2:	live2.sdp
RTSP port:	554
RTP port for video:	5556
RTCP port for video:	5557
RTP port for audio:	5558
RTCP port for audio:	5559

Multicast settings for stream 1:

Multicast settings for stream 2:

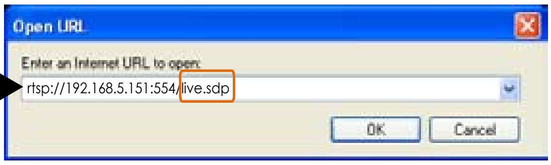
Authentication: Depending on your network security requirements, the Network Camera provides three types of security settings for streaming via RTSP protocol: disable, basic and digest.
If **basic** authentication is selected, the password is sent in plain text format; there can be potential risks of being intercepted. If **digest** authentication is selected, user credentials are encrypted in MD5 algorithm and thus provide better protection against unauthorized accesses.

The accessibility of the RTSP streaming for the three authentication modes are listed in the following table:

	Quick Time player	Real Player
Disable	O	O
Basic	O	O
Digest	O	X

Access name for stream 1 / Access name for stream 2: This Network camera supports dual streams simultaneously. The access name is used to differentiate the streaming source.
If you want to use a RTSP player to access the Network Camera, you have to set the video mode to MPEG-4, and use the following RTSP URL command to request a transmission of streaming data.

rtsp://<ip address>:<rtsp port>/<access name for stream1 or stream2>
For example, when the access name for stream 1 is set to live.sdp:
1. Launch a RTSP player.
2. Choose File > Open URL. An URL dialog box will pop up.
3. Type the URL command in the text box. For example:
4. The live video will be displayed in your player as below.



Open URL

Enter an Internet URL to open:

rtsp://192.168.5.151:554/live.sdp

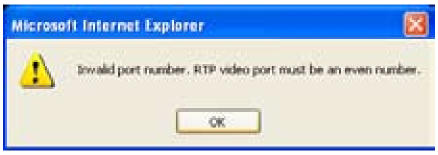
RTSP port /RTP port for video, audio/ RTCP port for video, audio
The RTSP (Real-Time Streaming Protocol) controls the delivery of streaming media. By default, the port number is set to 554.

■ The RTP (Real-time Transport Protocol) is used to deliver video and audio data to the clients. By default, the RTP port for video is set to 5556 and the RTP port for audio is set to 5558.

■ The RTCP (Real-time Transport Control Protocol) allows the Network Camera to transmit the data by monitoring Internet traffic volume. By default, the RTCP port for video is set to 5557 and the RTCP port for audio is set to 5559.

The five ports can be changed between 1025 and 65535. The RTP port must be an even number and the RTCP port is RTP port number plus one, and thus always be odd. When the RTP port changes, the RTCP port will change accordingly.

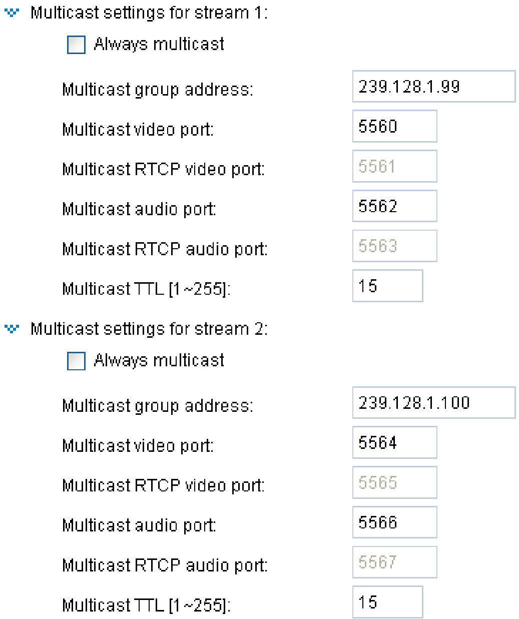
If the RTP ports are incorrectly assigned, the following warning message will display:



Microsoft Internet Explorer

Invalid port number. RTP video port must be an even number.

Multicast settings for stream 1 / Multicast settings for stream 2: Click the items to display the detailed configurations. Select the Always multicast to enable multicast for stream 1 or stream 2.



Multicast settings for stream 1:

□ Always multicast

Multicast group address:	239.128.1.99
Multicast video port:	5560
Multicast RTCP video port:	5561
Multicast audio port:	5562
Multicast RTCP audio port:	5563
Multicast TTL [1~255]:	15

Multicast settings for stream 2:

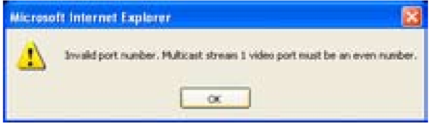
□ Always multicast

Multicast group address:	239.128.1.100
Multicast video port:	5564
Multicast RTCP video port:	5565
Multicast audio port:	5566
Multicast RTCP audio port:	5567
Multicast TTL [1~255]:	15

Unicast video transmission delivers a stream through point-to-point transmission; multicast, on the other hand, sends a stream to the multicast group address and allows multiple clients to acquire the stream at the same time by requesting a copy from the multicast group address. Therefore, multicast can effectively save Internet bandwidth.

The five ports can be changed between 1025 and 65535. The multicast RTP port must be an even number and the multicast RTCP port number is the multicast RTP port number plus one, and thus it is always be odd. When the multicast RTP port changes, the multicast RTCP port will change accordingly.

If the multicast RTP video ports are incorrectly assigned, the following warning message will display:

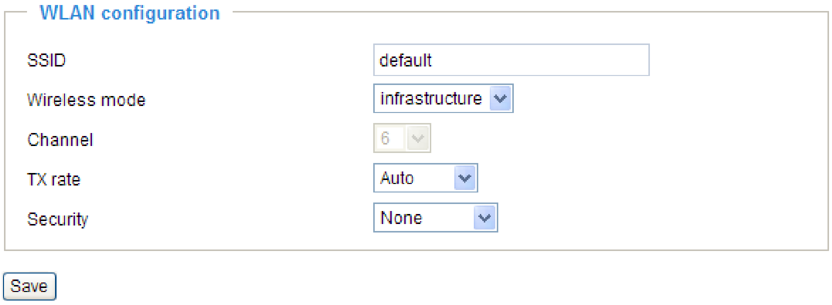


Microsoft Internet Explorer

Invalid port number. Multicast stream 1 video port must be an even number.

Multicast TTL [1~255]: The multicast TTL (Time to live) is the value that tells the router the range a packet can be forwarded.

Wireless LAN (PZ7132 only)



WLAN configuration

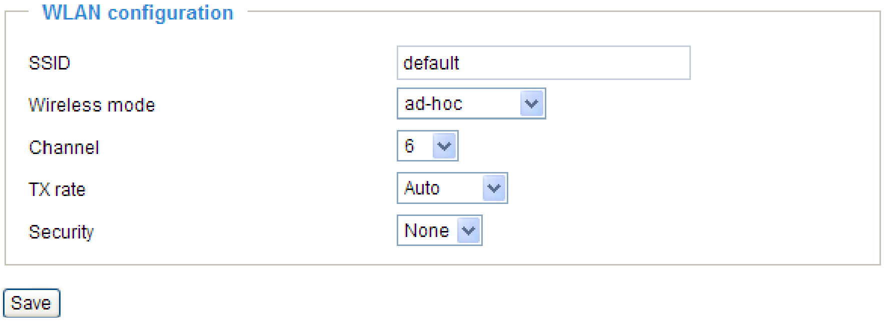
SSID	default
Wireless mode	infrastructure
Channel	6
TX rate	Auto
Security	None

SSID (Service Set Identifier): It is a name that identifies a wireless network. Access Points and wireless clients attempting to connect to a specific WLAN (Wireless Local Area Network) must use the same SSID. The default setting is default. Note: The maximum length of SSID is 32 single-byte characters and SSID can't be any of ", <, > and space character.

Wireless mode: Clicking on the pull-down menu to select from the following options:

Infrastructure: Make the Network Camera connect to the WLAN via an Access Point. (The default setting)

Ad-Hoc: Make the Network Camera connect directly to a host equipped with a wireless adapter in a peer-to-peer environment.



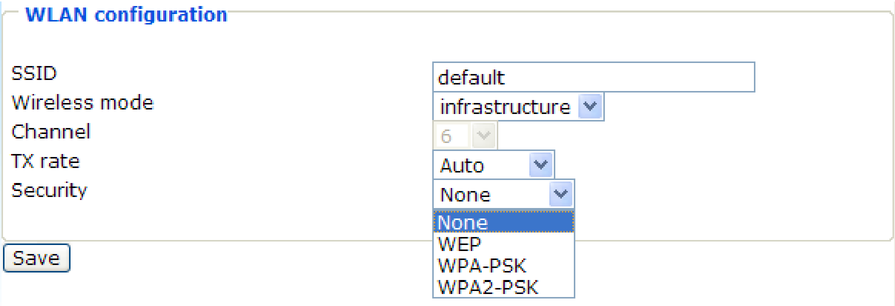
WLAN configuration

SSID	default
Wireless mode	ad-hoc
Channel	6
TX rate	Auto
Security	None

Channel: While in infrastructure mode, the channel is selected automatically to match the channel setting for the selected Access Point. In Ad-Hoc mode, the channel must be manually set to the same channel for each wireless adapter. The default channel setting depends on the installed region.

TX rate: This field is for selecting the maximum transmission rate on the network. The default setting is "auto", that is the Network Camera will try to connect to the other wireless device with highest transmitting rate.

Security: Select the data encrypt method. There are four types including none, WEP, WPA-PSK, and WPA2-PSK.

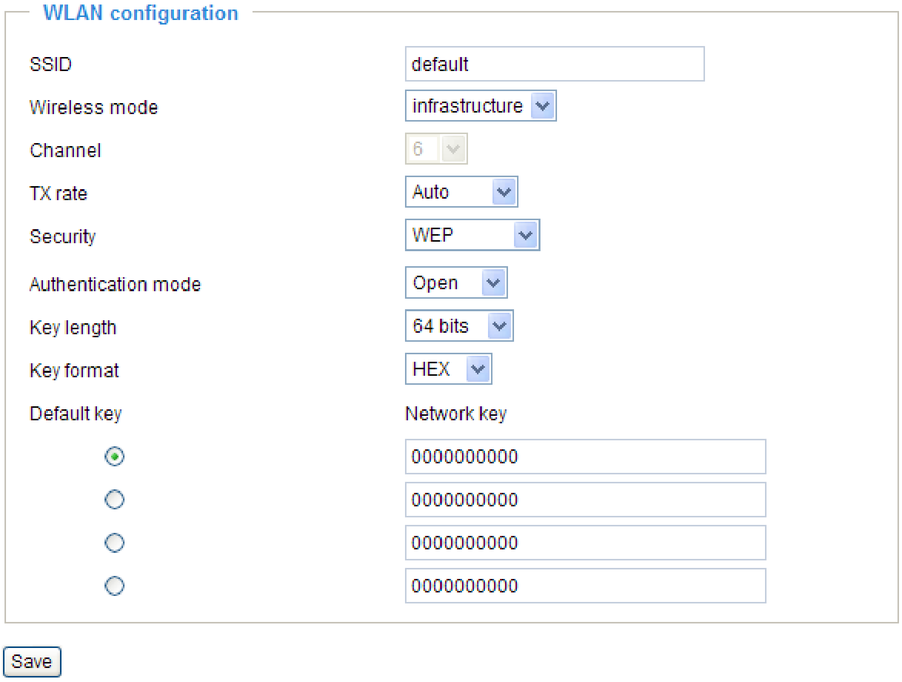


WLAN configuration

SSID	default
Wireless mode	infrastructure
Channel	6
TX rate	Auto
Security	None

1. None: No data encryption.

2. WEP (Wired equivalent Privacy): It allows communication only with other devices with identical WEP settings.



WLAN configuration

SSID	default
Wireless mode	infrastructure
Channel	6
TX rate	Auto
Security	WEP
Authentication mode	Open
Key length	64 bits
Key format	HEX
Default key	Network key
●	0000000000
○	0000000000
○	0000000000
○	0000000000

■ Authentication Mode: Choose one of the following modes. Open is the default setting.
Open – communicates the key across the network.
Shared – allows communication only with other devices with identical WEP settings.

■ Key length: The administrator can select the key length among 64 or 128 bits.
64 bits is the default setting.

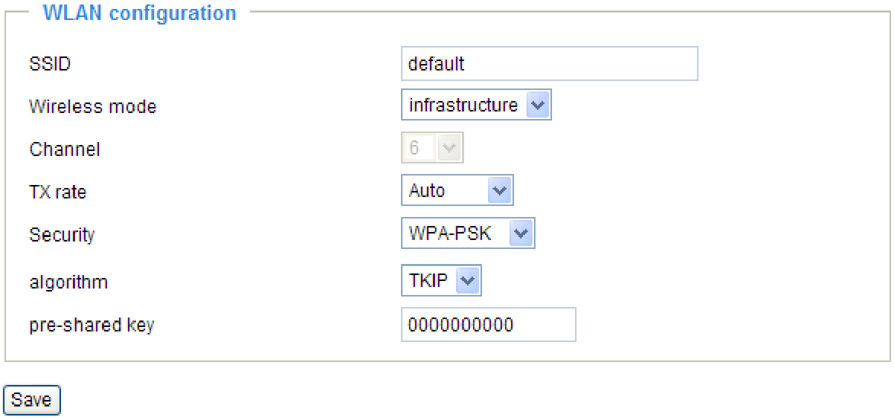
■ Key format: Hexadecimal or ASCII. HEX is the default setting.
HEX digits consist of the numbers 0~9 and the letters A-F.
ASCII is a code for representing English letters as numbers from 0-127 except “, <, > and space characters that are reserved.

■ Network Key: Enter a key in either hexadecimal or ASCII format.
You can select different key length, and acceptable input length is listed as following:
64 bits key length: 10 Hex digits or 5 characters.
128 bites key length: 26 Hex digits or 13 characters.

NOTE

► *When 22(“), 3C(<) or 3E(>) are input in network key, the key format can’t be changed to ASCII format.*

3. WPA-PSK: Use WPA (Wi-Fi Protected Access) pre-shared key.



WLAN configuration

SSID	default
Wireless mode	infrastructure
Channel	6
TX rate	Auto
Security	WPA-PSK
algorithm	TKIP
pre-shared key	0000000000

More secure than WEP, the Wi-Fi Alliance developed WPA (Wi-Fi Protected Access) in 2003 to address WEP's weaknesses. Improvements included TKIP, which changes the encryption key for each data transmission.

■ Algorithm: Choosing one of the following algorithm for WPA-PSK and WPA2-PSK modes.

TKIP (Temporal Key Integrity Protocol): A security protocol used in the IEEE 802.11 wireless networks. TKIP is a “wrapper” that goes around the existing WEP encryption. TKIP comprises the same encryption engine and RC4 algorithm defined for WEP. However, the key used for encryption in TKIP is 128 bits long. This solves the first problem of WEP: a too-short key length. (From Wikipedia)

AES (Advanced Encryption Standard): In cryptography, the Advanced Encryption Standard (AES), also known as Rijndael, is a block cipher adopted as an encryption standard by the U.S. government. As of 2006, AES is one of the most popular algorithms used in symmetric key cryptography. (From Wikipedia)

■ Pre-shared Key: Entering a key in ASCII format. The length of the key is 8 ~ 63.

4. WPA2-PSK: Use WPA2 pre-shared key.

The advanced protocol, certified through Wi-Fi Alliance's WPA2 program, implements the mandatory elements of 802.11i. In particular, it introduces a new AES-based algorithm, CCMP, that is considered fully secure. From March 13, 2006, WPA2 certification is mandatory for all new devices wishing to be certified by the Wi-Fi Alliance as “Wi-Fi CERTIFIED.” (From Wikipedia)

NOTE

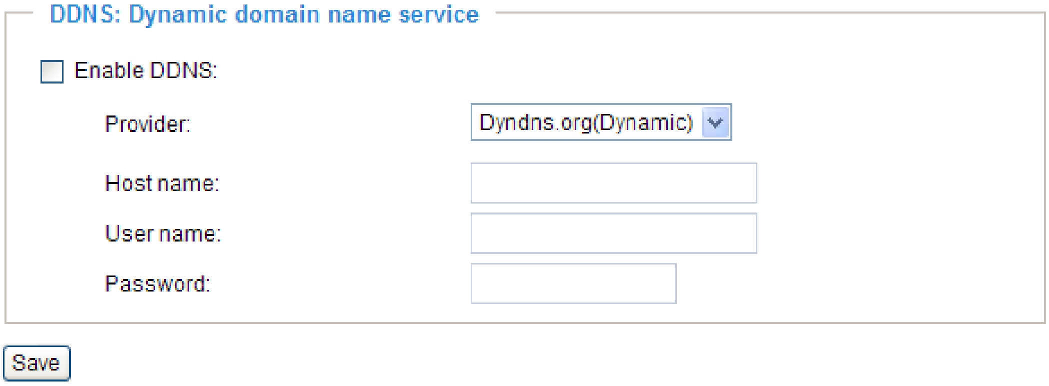
► *After wireless configurations are completed, click **Save** and the camera will reboot. Wait for the live image is reloaded to your browser. For VIVOTEK 7000-series cameras, you have to unplug the power cable and Ethernet cable from the camera; then re-plug the power cable to the camera. The camera will switch to wireless mode.*

► *Some invalid settings may cause the system failing to respond. Change the Configuration only if necessary and consult with your network supervisor or experienced users for correct settings. Once the system has lost contact, please refer to Maintenance on page 84 for reset and restore procedures.*

DDNS

This section explains how to configure dynamic domain name service for the Network Camera. DDNS is a service that allows your Network Camera, especially when assigned with a dynamic IP address, to have a fixed host and domain name.

DDNS: Dynamic domain name service



DDNS: Dynamic domain name service

□ Enable DDNS:

Provider: Dyndns.org(Dynamic)

Host name:

User name:

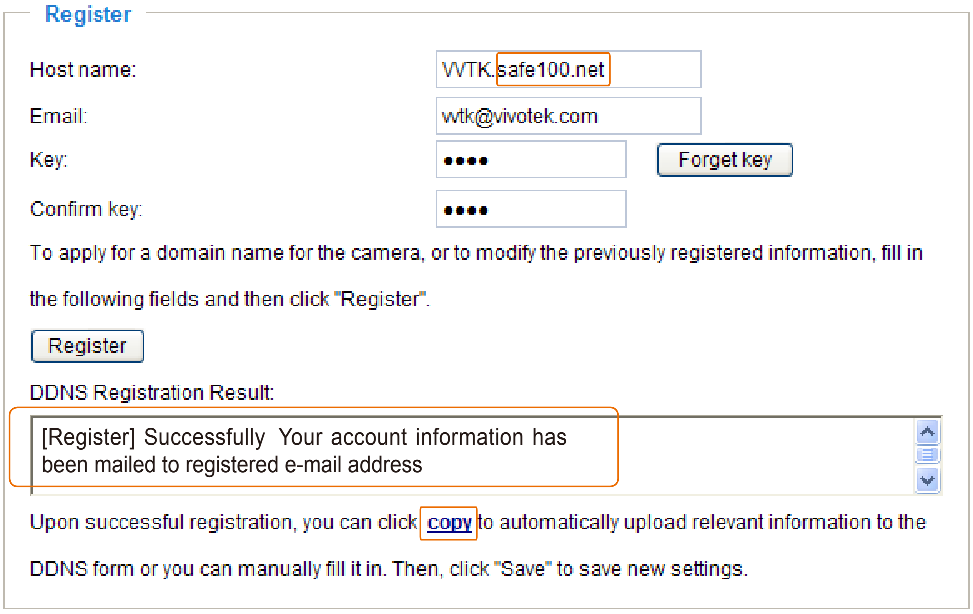
Password:

Enable DDNS: Select this option to enable the DDNS setting.

Provider: Select a DDNS provider from the Provider drop-down list.
VIVOTEK offers **Safe100.net**, a free dynamic domain name service to VIVOTEK customers. It is recommended that you register **Safe100.net** to access VIVOTEK's network camera from the Internet. Additionally, we offer other DDNS providers, such as Dyndns.org (Dynamic), Dyndns.org (Custom), TZO.com, DHS.org, CustomSafe100, dyn-interfree.it.
Note that before utilizing this function, please apply a dynamic domain account first.

■ Safe100.net

1. In the DDNS column, select **Safe100.net** from the drop-down list. Click **I accept** after reviewing the terms of the Service Agreement.
2. In the Register column, fill in the Host name (xxxx.safe100.net), Email, Key and Confirm Key, and then click **Register**. After a host name has been successfully created, a successful message will show in the DDNS Registration Result column.



Register

Host name: VVTK.safe100.net

Email: wtk@vivotek.com

Key: ••••

Confirm key: ••••

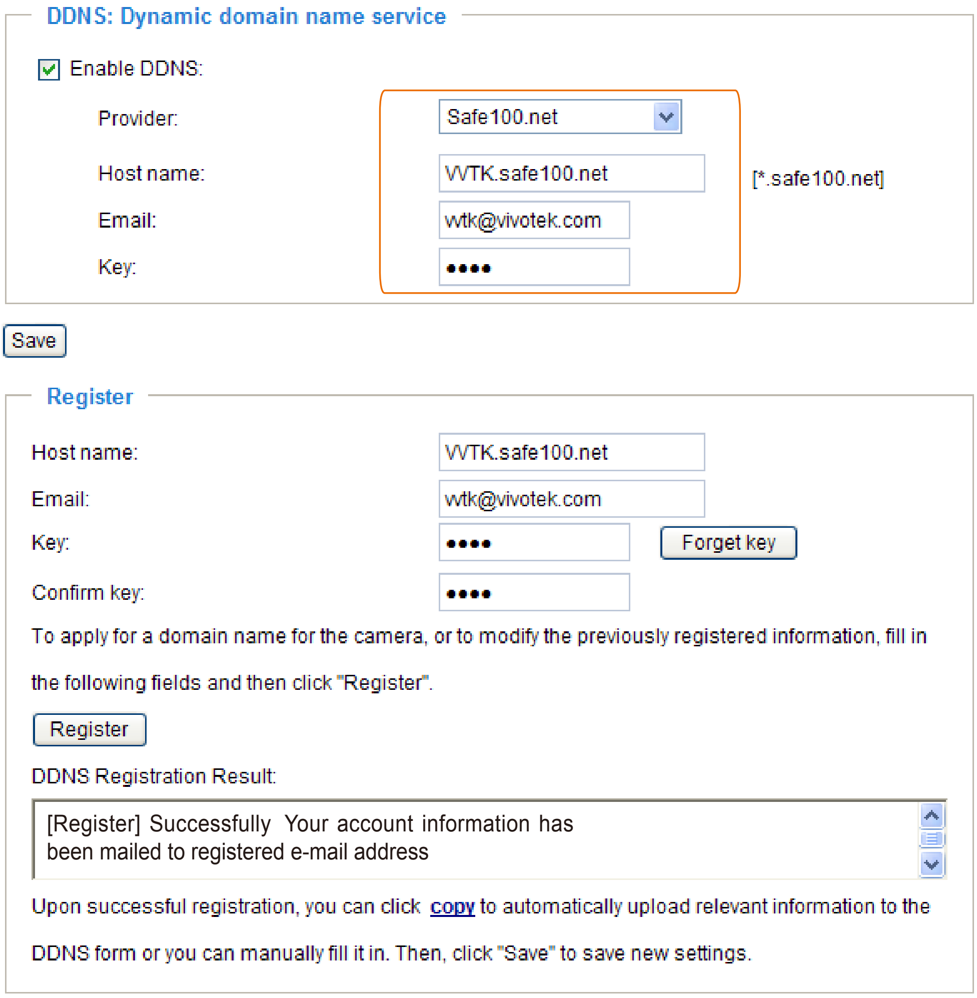
To apply for a domain name for the camera, or to modify the previously registered information, fill in the following fields and then click "Register".

DDNS Registration Result:

[Register] Successfully Your account information has been mailed to registered e-mail address

Upon successful registration, you can click copy to automatically upload relevant information to the DDNS form or you can manually fill it in. Then, click "Save" to save new settings.

3. Click **Copy** and all the registered information will automatically be uploaded to the corresponding fields in the DDNS column on the top of the page as the picture shows.



DDNS: Dynamic domain name service

☑ Enable DDNS:

Provider: Safe100.net

Host name: VVTK.safe100.net [*.safe100.net]

Email: vtk@vivotek.com

Key: ●●●●

Register

Host name: VVTK.safe100.net

Email: vtk@vivotek.com

Key: ●●●●

Confirm key: ●●●●

To apply for a domain name for the camera, or to modify the previously registered information, fill in the following fields and then click "Register".

DDNS Registration Result:

[Register] Successfully Your account information has been mailed to registered e-mail address

Upon successful registration, you can click copy to automatically upload relevant information to the DDNS form or you can manually fill it in. Then, click "Save" to save new settings.

4. Select Enable DDNS and then click **Save** to take effect.

■ CustomSafe100

VIVOTEK offers documents to establish CustomSafe100 DDNS server for distributors and system integrators. You can use CustomSafe100 to register a dynamic domain name if your distributor or system integrators offer such services.

1. In the DDNS column, select CustomSafe100 from drop-down list.
2. In the Register column, fill in the Host name, Email, Key and Confirm Key; then click **Register**. After a host name has been successfully created, you will see a successful message in the DDNS Registration Result column.
3. Click **Copy** and all the registered information will be uploaded to the corresponding fields in the DDNS column.
4. Select Enable DDNS and then click **Save** to take effect.

Forget key: Click this button if you forget the key of Safe100.net or CustomSafe100. Your account information will be sent to your email address.

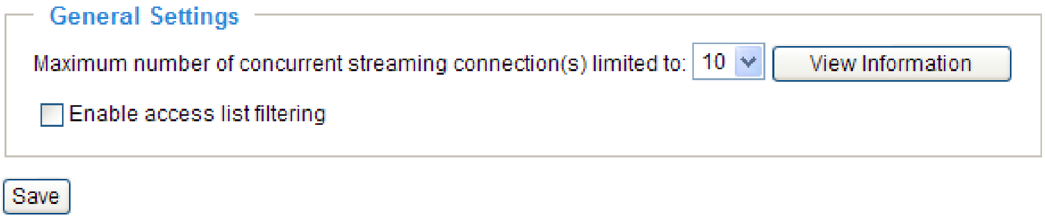
Refer to the following links to apply a dynamic domain account when selecting other DDNS providers:

■ Dyndns.org (Dynamic) / Dyndns.org (Custom): visit http://www.dyndns.com/
■ TZO.com: visit http://www.tzo.com/
■ DHS.org: visit http://www.dhs.org/
■ dyn-interfree.it: visit http://dyn-interfree.it/

Access list Advanced mode

This section explains how to control the access permission by checking the client PC’s IP addresses.

General Settings



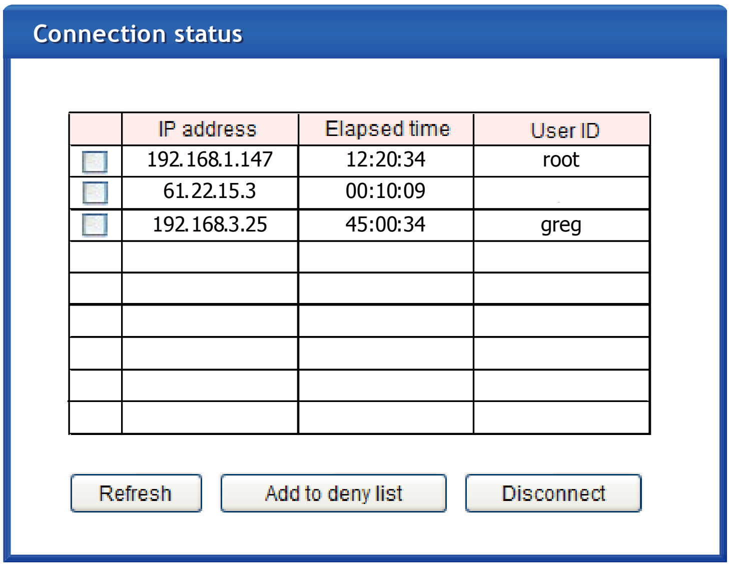
General Settings

Maximum number of concurrent streaming connection(s) limited to: 10

□ Enable access list filtering

Maximum number of concurrent streaming connection(s) limited to: Simultaneous live viewing for 1~10 clients (including stream 1 and stream 2). The default value is 10. If you modify the value and then click **Save** to enable the setting, all current connections will be disconnected and then automatically try to re-link again (IE Explore or Quick Time Player).

View Information: Click this button will pop up a connection status window, showing a list of current connections. For example:



Connection status

	IP address	Elapsed time	User ID
□	192.168.1.147	12:20:34	root
□	61.22.15.3	00:10:09	
□	192.168.3.25	45:00:34	greg

■ IP address: Current connections.

■ Elapsed time: How much time the client link to the webpage.

■ User ID: If the administrator set password for the webpage, the clients have to enter the user name and password to get access to the live video. The user name will show on the column of User ID. If the administrator allows clients to link to the webpage without user name and password, the column of user ID will be empty.

There are some situations which allows clients to get access to the live video without user name and password:

1. The administrator does not setup root password. For more information about how to setup root password and manage user account, please refer to Security on page 27.
2. The administrator has setup root password, but set **RTSP Authentication** “disable“. So clients can use RTSP players to link to the live video without user name and password. For more information about **RTSP Authentication,** please refer to RTSP Streaming on page 42.
3. The administrator has setup root password, but allows anonymous viewing. So clients can link to the live video without user name and password. For more information about **Allow Anonymous Viewing,** please refer to Security on page 27.

- Refresh: Click this button will refresh all current connections.

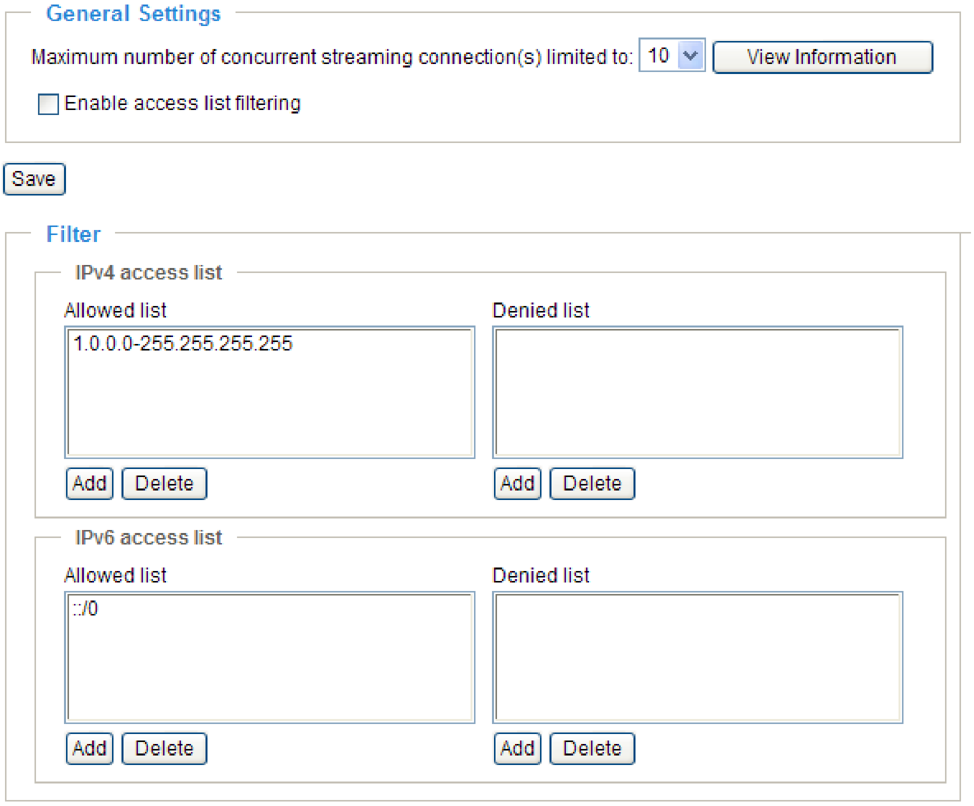
- Add to deny list: You can check some items on the connection status list, and then click this button to add them to the denied list. Please note that those checked connections will only be disconnected temporarily, but will automatically try to re-link again (IE Explore or Quick Time Player). If you want to enable the denied list, please check **Enable access list filtering** and click **Save** in the first column.

- Disconnect: If you want to break off some current connections, please check them and click this button. Please note that those checked connections will only be disconnected temporarily, but will automatically try to re-link again (IE Explore or Quick Time Player).

Enable access list filtering: Check this item and click **Save** if you want to enable the access list filtering function.

Filter

There are two lists for permission control: Allowed list and Denied list. Only those clients whose IP addresses are in the Allowed list and not in the Denied list can access the Network Camera. Please note that the IPv6 access list column will not be displayed unless you enable IPv6 in Network page. For more information about **IPv6 settings**, please refer to page 37 for detailed information.



General Settings

Maximum number of concurrent streaming connection(s) limited to: 10

□ Enable access list filtering

Filter

IPv4 access list

Allowed list: 1.0.0.0-255.255.255.255

Denied list:

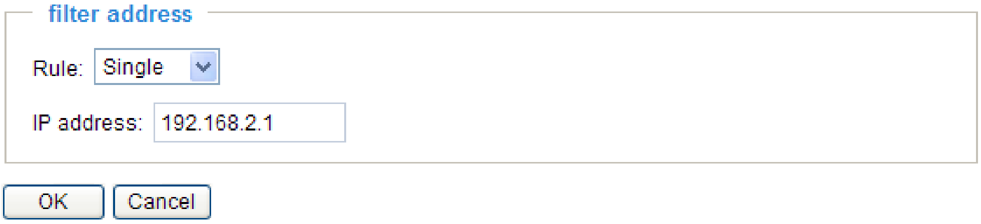
IPv6 access list

Allowed list: ::/0

Denied list:

- Add a rule to Allowed/Denied list: Click **Add** to add a rule to Allowed/Denied list.

There are three types of rules for user to set up:
Single: This rule is for user to add an IP address to Allowed/Denied list.
For example:

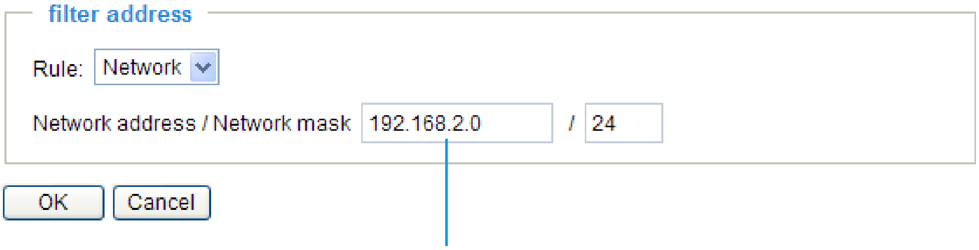


filter address

Rule: Single

IP address: 192.168.2.1

Network: This rule is for user to assign a Network address and corresponding subnet mask to Allow/Deny list.
For example:



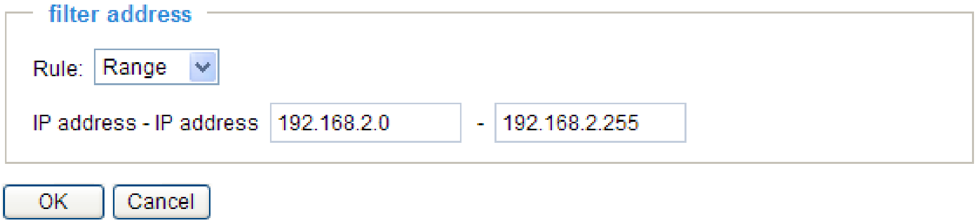
filter address

Rule: Network

Network address / Network mask 192.168.2.0 / 24

IP address 192.168.2.x will be bolcked.

Range: This rule is for user to assign a range of IP address to Allow/Deny list. This rule is only applied to IPv4.
For example:



filter address

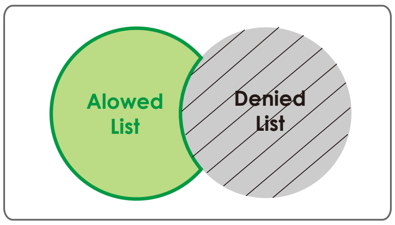
Rule: Range

IP address - IP address 192.168.2.0 - 192.168.2.255

■ Delete Allowed/Denied list:
In the Delete allowed list or Delete denied list column, select a list from the list and then click **Delete** to delete it.

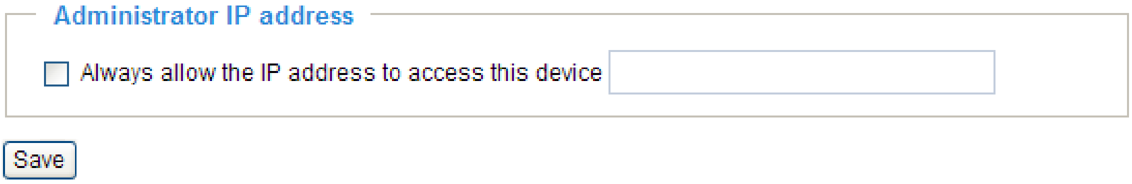
NOTE

► *For example, when the range of allowed list is set from 1.1.1.0 to 192.255.255.255 and the range of denied list is set from 1.1.1.0 to 170.255.255.255, Only users' IP located between 171.0.0.0 and 192.255.255.255 can access the Network Camera.*



Administrator IP address

Always allow the IP address to access this device: You can check this item and add the Administrator's IP address in this field to make sure the Administrator can always connect to the device.



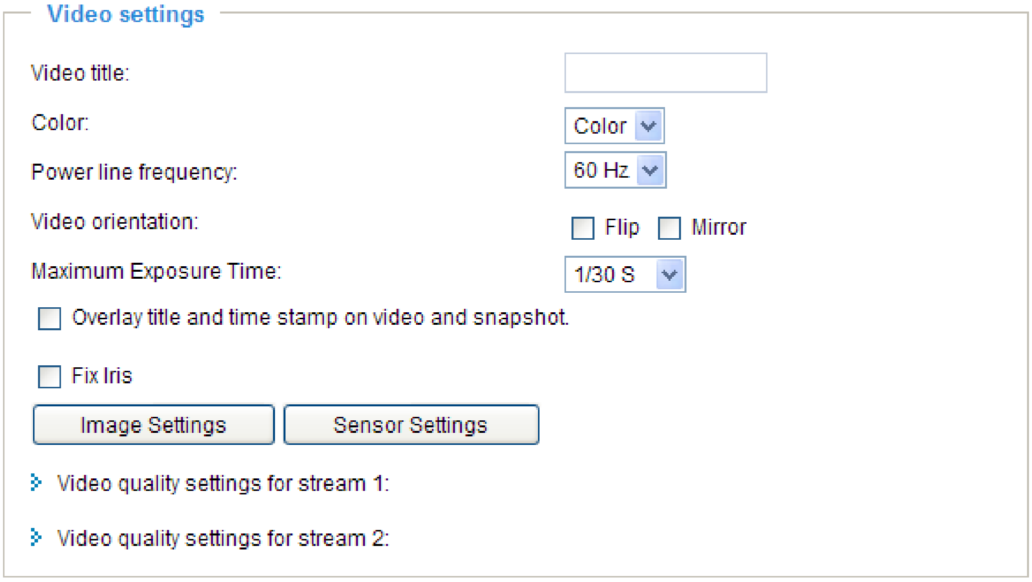
Administrator IP address

□ Always allow the IP address to access this device

Audio and video

This section explains how to configure audio and video performances of the Network Camera. It is composed of the following two columns: Video settings and Audio settings.

Video Settings



Video settings

Video title:

Color: Color

Power line frequency: 60 Hz

Video orientation: □ Flip □ Mirror

Maximum Exposure Time: 1/30 S

□ Overlay title and time stamp on video and snapshot.

□ Fix Iris

Video quality settings for stream 1:

Video quality settings for stream 2:

Video title: Enter a name that will be displayed on the title bar of the live video.

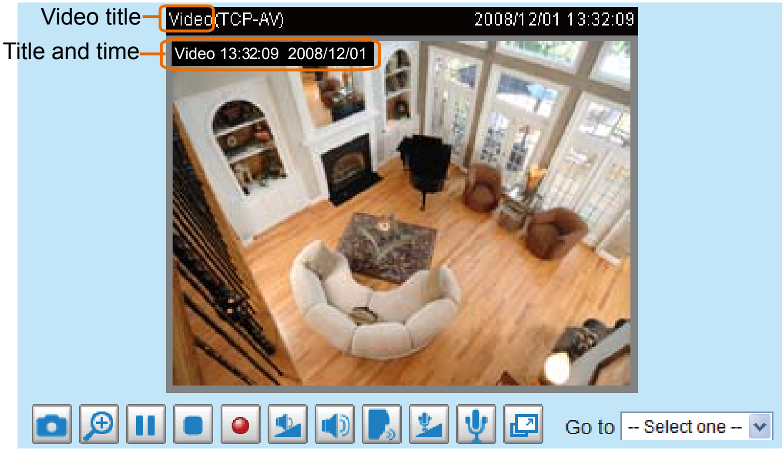
Color: Select to display colorful or black/white video streams.

Power line frequency: Set the power line frequency in consistent with local utility settings to eliminate uncomfortable image flickering associated with fluorescent lights. Note that after the power line frequency is changed, it is required to disconnect and reconnect the power cord of the Network Camera in order for the new setting to take effect.

Video orientation: Flip--vertically reflect the display of the live video; Mirror--horizontally reflect the display of the live video. Select both options if the Network Camera is installed upside-down (ex. on the ceiling) to correct the image orientation.

Maximum Exposure Time: 1/120 S, 1/60 S, 1/30 S, 1/15 S, 1/5 S, and Auto.

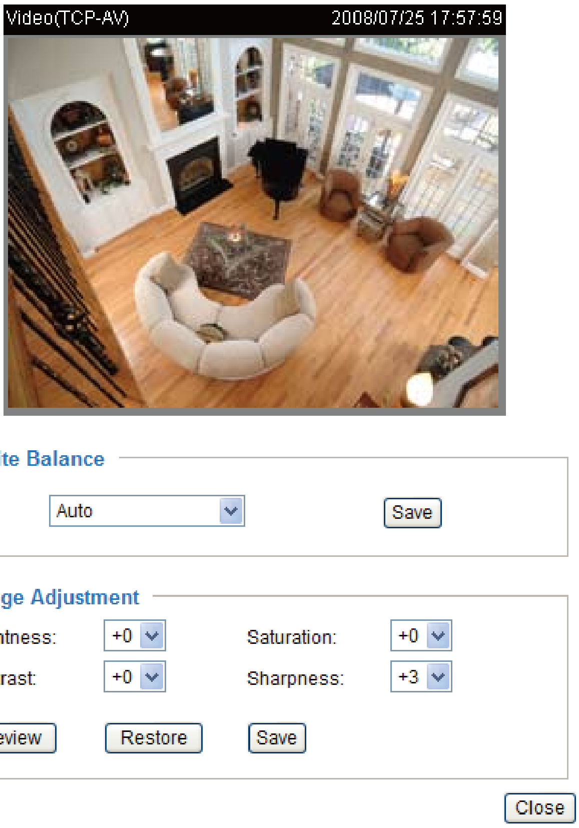
Overlay title and time stamp on video: Select this option to place the video title and time on video streams.
Note that when the frame size is set to 176 x 144 as the right picture below, only time will be stamped on video streams.



Fix iris Advanced mode : Select this item to set up the iris at the maximum value; then adjust the zoom factor and focus range.

Image Settings Advanced mode

Click **Image settings** to open the Image Settings page. In this page, you can tune White balance, Brightness, Saturation, Contrast, and Sharpness for video compensation.



White Balance

Auto

Image Adjustment

Brightness: +0
Saturation: +0
Contrast: +0
Sharpness: +3

White balance: Adjust the value for best color temperature.

■ Auto

The Network Camera automatically adjusts the color temperature of light in response to different light sources. The white balance setting defaults to Auto and works well in most situations.

■ Keep current value

Follow the steps below to manually set the white balance to compensate for the ambient lighting conditions.

1. Set the White balance to Auto and click **Save**.
2. Place a sheet of white paper in front of the lens; then allow the Network Camera to adjust the color temperature automatically.
3. Select Keep current value to confirm the setting while the white balance is being measured.
4. Click **Save** to take effect.

Image Adjustment

■ Brightness: Adjust the image brightness level, which ranges from -5 to +5. The default value is set to 0.

■ Saturation: Adjust the image saturation level, which ranges from -5 to +5. The default value is set to 0.

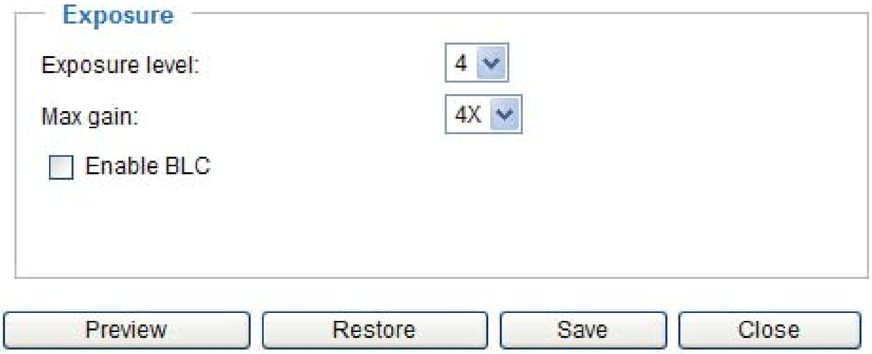
■ Contrast: Adjust the image contrast level, which ranges from -5 to +5. The default value is set to 0.

■ Sharpness: Adjust the image sharpness level, which ranges from -3 to +3. The default value is set to 0.

You can click **Preview** to fine-tune the image, or click **Restore** to recall the original settings without incorporating the changes. When completed with the settings on this page, click **Save** to take effect and click **Close** to quit the page.

Sensor Settings Advanced mode

Click Sensor Settings to open the Sensor Settings page. In this page, you can set the maximum exposure time, exposure level, AGC, and WDR (Wide Dynamic Range) settings.
You can configure two sets of sensor settings: one for normal situation; the other for special situation, such as day/night/schedule mode.



Exposure

Exposure level: 4

Max gain: 4X

□ Enable BLC

Exposure

■ Exposure level: You can manually set up the Exposure level, which ranges from 1 to 8 (dark to bright). The default value is 4.

■ Max gain (Auto Gain Control): You can manually set up the AGC level (4X or 8X). The default value is 4X.

■ Enable BLC (Back Light Compensation)
Enable it when the object is too dark or too bright to recognize. It allows the camera to adjust to the best light conditions in any environment and automatically give the necessary light compensation.

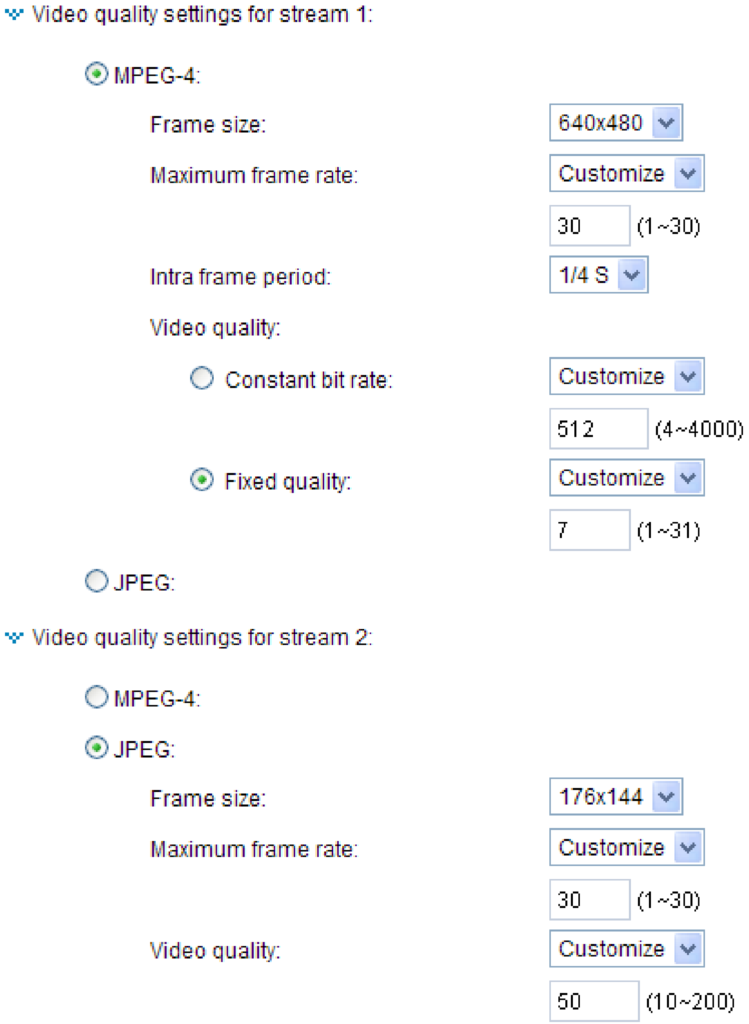
You can click **Preview** to fine-tune the image, or click **Restore** to recall the original settings without incorporating the changes. When completed with the settings on this page, click **Save** to take effect and click **Close** to quit the page.

Video quality settings for stream 1 / stream 2 Advanced mode

The Network Camera offers two choices of video compression standards for real-time viewing, so you can choose MPEG-4 or MJPEG for dual streams.

Click the items to display the detailed configurations. You can set up two seperate streams for the Network Camera for different viewing devices. For example, set a smaller frame size and a lower bit rate for remote viewing on mobile phones; or set a larger video size and a higher bit rate for live viewing on web browsers.

If **MPEG-4** mode is selected, it is streamed in RTSP protocol. There are four dependent parameters provided in MPEG-4 mode for video performance adjustment.



Video quality settings for stream 1:

● MPEG-4:

Frame size: 640x480

Maximum frame rate: Customize

30 (1~30)

Intra frame period: 1/4 S

Video quality:

○ Constant bit rate: Customize

512 (4~4000)

● Fixed quality: Customize

7 (1~31)

○ JPEG:

Video quality settings for stream 2:

○ MPEG-4:

● JPEG:

Frame size: 176x144

Maximum frame rate: Customize

30 (1~30)

Video quality: Customize

50 (10~200)

■ Frame size
Select the video size. Note that a larger frame size takes up more bandwidth. The frame sizes are selectable in the following resolutions: 176 x 144, 320 x 240 and 640 x 480.

■ Maximum frame rate
This limits the maximal refresh frame rate per second. Set the frame rate higher for a smoother video quality.

If the power line frequency is set to 50Hz, the frame rates are selectable at the following rates: 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps and 25fps. If the power line frequency is set to 60Hz, the frame rates are selectable at the following rates: 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, 25fps and 30fps. You can also select **Customize**, and manually enter a value.

■ Intra frame period
Determine how often to plant an I frame. The shorter the duration, the more likely you will get a better video quality, but at the cost of higher network bandwidth consumption. Select the intra frame period from the following duration: 1/4 second, 1/2 second, 1 second, 2 seconds, 3 seconds and 4 seconds.

■ Video quality
A complex scene generally produces larger file size, meaning that higher bandwidth will be needed for data transmission. Therefore, if **Constant bit rate** is selected, the bandwidth utilization is fixed at a selected level, resulting in mutable video quality performances. The bit rates are selectable at the following rates: 20Kbps, 30Kbps, 40Kbps, 50Kbps, 64Kbps, 128Kbps, 256Kbps, 512Kbps, 768Kbps, 1Mbps, 2Mbps, 3Mbps and 4Mbps. You can also select **Customize**, and manually enter a value.

On the other hand, if **Fixed quality** is selected, all frames are transmitted with the same quality; bandwidth utilization is therefore unpredictable. The video qualities are selectable at the following settings: Medium, Standard, Good, Detailed and Excellent. You can also select **Customize**, and manually enter a value.

If **JPEG** mode is selected, the Network Camera continuously sends JPEG images to the clients, producing dynamic effects similar to movies. Every single JPEG image transmitted guarantees the same image quality, which in turn comes at the expense of variable bandwidth usage. And because the media contents are a combination of JPEG images, no audio data is transmitted to the clients. There are three dependent parameters provided in MPEG-4 mode for video performance adjustment.

■ Frame size
Select the video size. Note that a larger frame size takes up more bandwidth. The frame sizes are selectable in the following resolutions: 176 x 144, 320 x 240 and 640 x 480.

■ Maximum frame rate
This limits the maximal refresh frame rate per second. Set the frame rate higher for a smoother video quality.

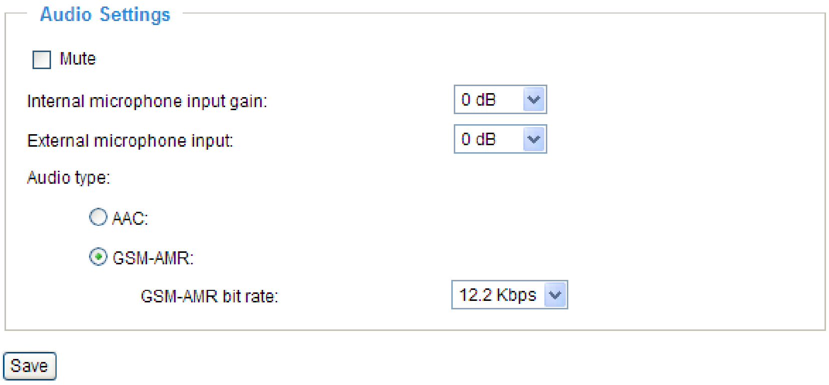
If the power line frequency is set to 50Hz, the frame rates are selectable at the following rates: 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps and 25fps. If the power line frequency is set to 60Hz, the frame rates are selectable at the following rates: 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, 25fps and 30fps. You can also select **Customize**, and manually enter a value.

■ Video quality
The video qualities are selectable at the following settings: Medium, Standard, Good, Detailed and Excellent. You can also select **Customize**, and manually enter a value.

NOTE

► *The value of video quality and fixed quality refers to the **compression rate**, so the lower the value will produce the higher quality.*

Audio settings



Audio Settings

☐ Mute

Internal microphone input gain: 0 dB

External microphone input: 0 dB

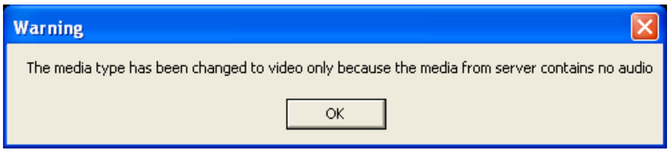
Audio type:

○ AAC:

● GSM-AMR:

GSM-AMR bit rate: 12.2 Kbps

Mute: Select this option to disable audio transmission from the Network Camera to all clients. Note that if mute mode is turned on, no audio data will be transmitted to all clients even though the audio transmission is enabled in the Client Settings page. In that case, the following message is displayed.



Warning

The media type has been changed to video only because the media from server contains no audio

Internal microphone input gain: Select the gain of the internal audio input according to ambient conditions. Adjust the gain from +21 db (most sensitive) ~ -33 db (least sensitive).

External microphone input: Select the gain of the external audio input according to ambient conditions. Adjust the gain from +21 db (most sensitive) ~ -33 db (least sensitive).

Audio type: Select audio codec AAC or GSM-AMR and the bit rate.

■ AAC targets at performing good sound quality at the cost of higher bandwidth consumption. The bit rates are selectable at the following rates: 16Kbps, 32Kbps, 48Kbps, 64Kbps, 96Kbps and128Kbps.

■ GSM-ARM is designed to optimize speech quality and requires less bandwidth. The bit rates are selectable at the following rates: 4.75Kbps, 5.15Kbps, 5.90Kbps, 6.7Kbps, 7.4Kbps, 7.95Kbps, 10.2Kbps and 12.2Kbps.

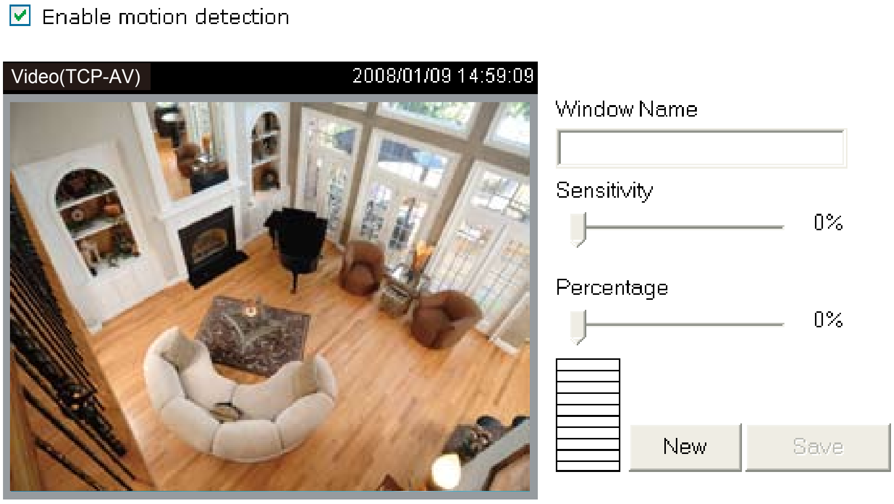
When completed with the settings on this page, click **Save** to take effect.

NOTE

► *The Network Camera offers two inputs to capture audio - internal microphone or external microphone. The internal/external microphone switch is located on the back panel of the Network Camera.*

Motion detection

This section explains how to configure the Network Camera to enable motion detection. A total of three motion detection windows can be configured.



☑ Enable motion detection

Video(TCP-AV) 2008/01/09 14:59:09

Window Name:

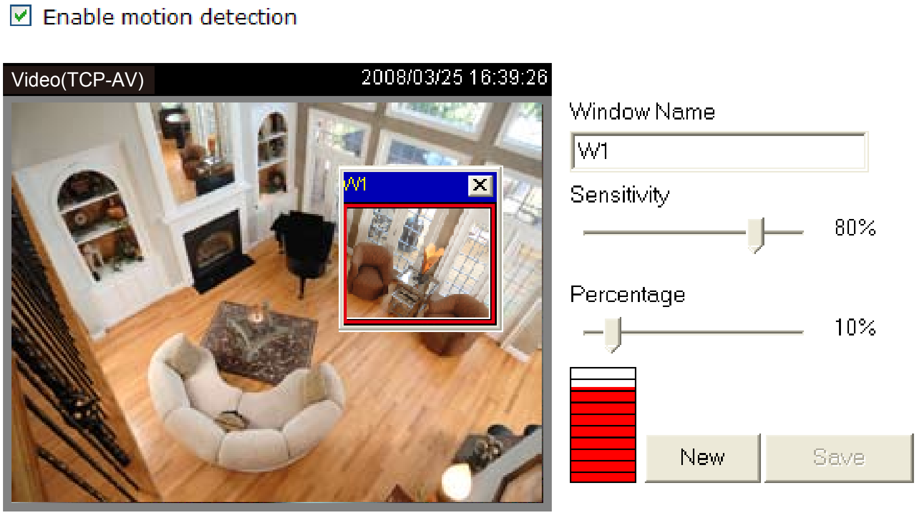
Sensitivity: 0%

Percentage: 0%

Follow the steps below to enable motion detection:

1. Click **New** to add a new motion detection window.
2. In the Window Name text box, enter a descriptive name for the motion detection window.
   ■ To move and resize the window, drag-drop the window.
   ■ To delete window, click X at top right of the window.
3. Define the sensitivity to moving objects and the space ratio of all alerted pixels by moving the Sensitivity and Percentage slider bar.
4. Click **Save** to take effect.
5. Check **Enable motion detection** to enable this function.

For example:



☑ Enable motion detection

Video(TCP-AV) 2008/03/25 16:39:26

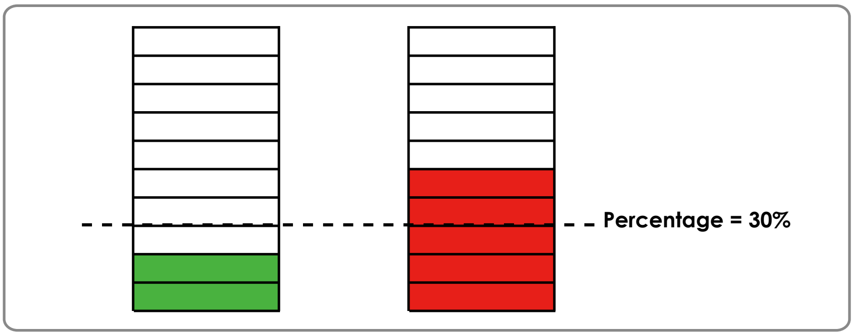
Window Name: W1

Sensitivity: 80%

Percentage: 10%

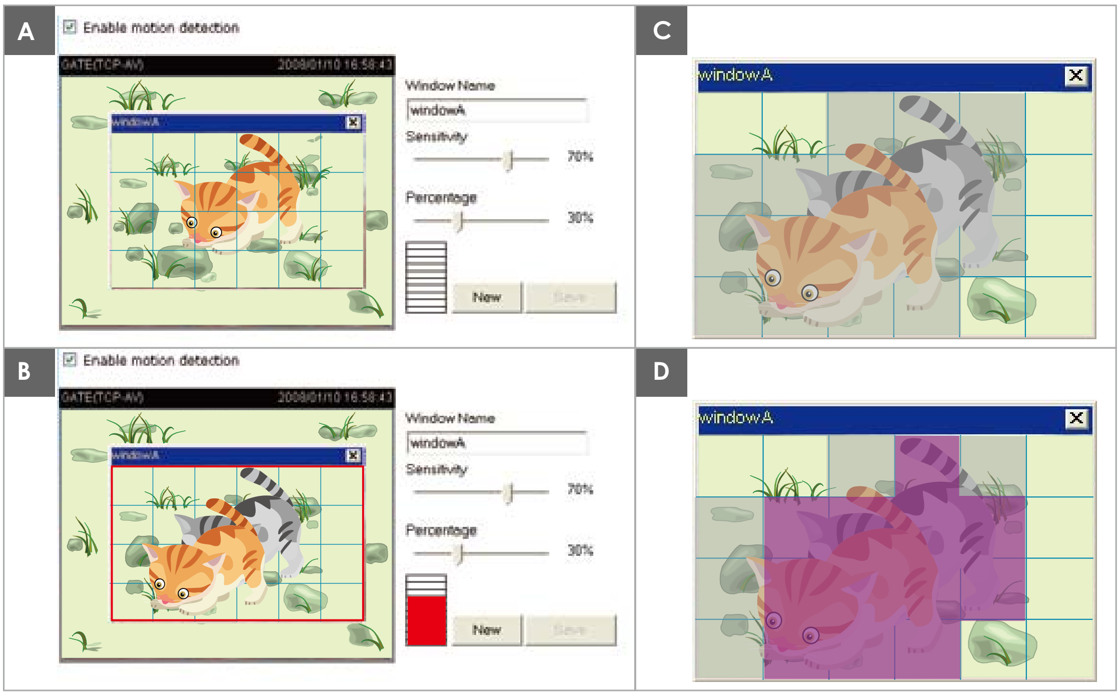
The Percentage Indicator will rise or fall depending on the image variation. When motions are detected by the Network Camera and are judged to exceed the defined threshold, a red bar rises. Meanwhile, the motion detection window will be outlined in red. Photos or videos can be captured instantly and configured to send to the remote server (Email, FTP) by utilizing this feature as a trigger source. For more information about how to plot an event, please refer to Application on page 66.

A green bar indicates that even though motions are detected, the event will not be triggered because the image variations are still falling under the defined threshold.



NOTE

► *How does motion detection work?*



☑ Enable motion detection

Window Name: windowA

Sensitivity: 70%

Percentage: 30%

There are two parameters for setting the motion detection: Sensitivity and Percentage. In the illustration above, frame A and frame B are two sequential images. Pixel differences between the two frames are detected and highlighted in gray (frame C), and will be compared with the sensitivity setting. Sensitivity is a value that expresses the sensitivity to moving objects. Higher sensitivity settings are expected to sense a slight movement while smaller sensitivity settings tend to neglect it. When the sensitivity is set to 70%, the Network Camera defines the pixels in the purple areas as "alerted pixels" (frame D).

Percentage is a value that expresses the proportion of "alerted pixels" to all pixels in the motion detection window. In this case, 50% of pixels are identified as "alerted pixels". When the percentage is set to 30%, the motions are judged to exceed the defined threshold; therefore, the motion window will be outlined in red.

For applications that require higher security management, it is suggested to set higher sensitivity settings and smaller percentage values.

Camera control

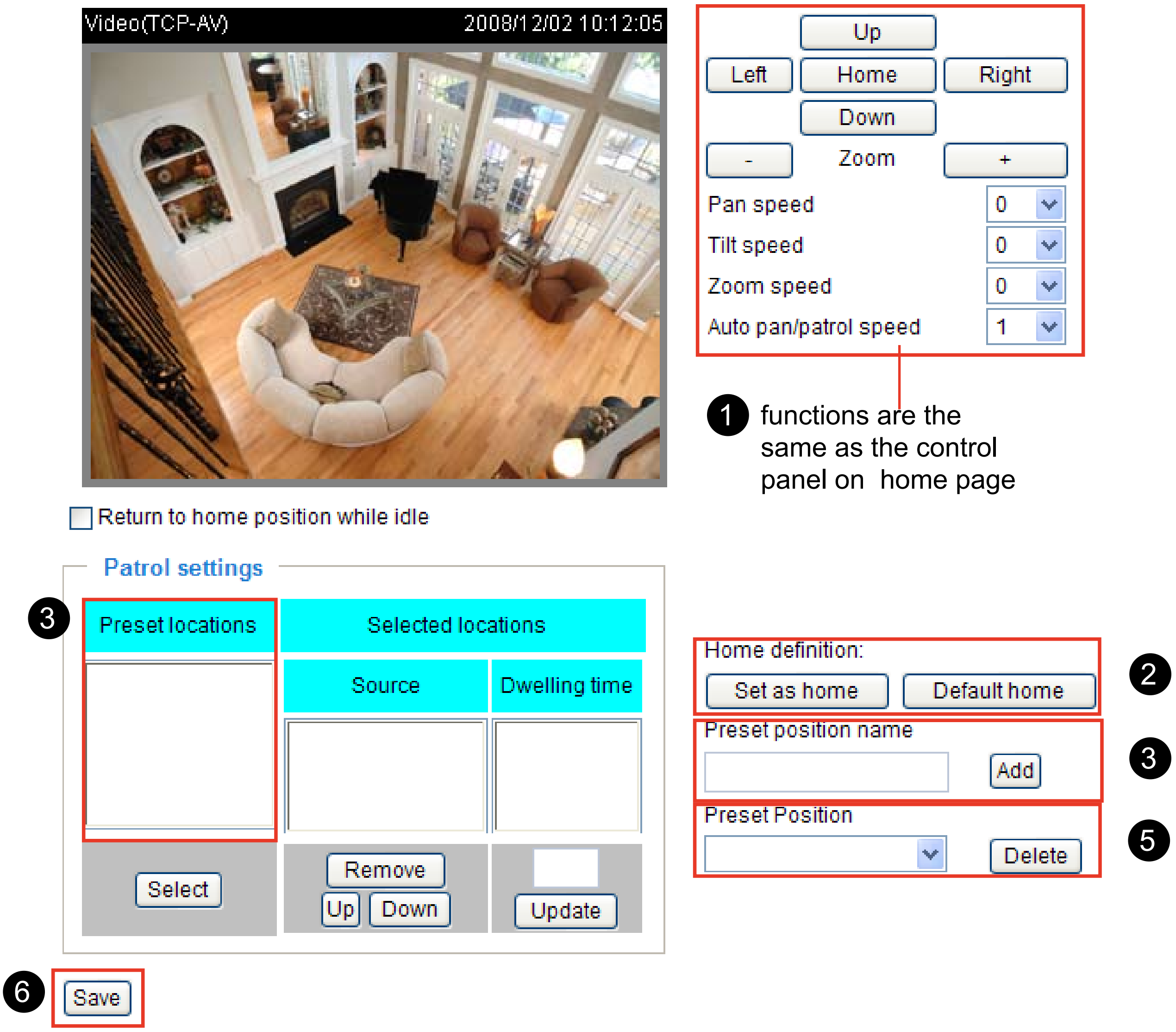
This section explains how to control the Network Camera's Pan/Tilt/Zoom/Focus operation by a control panel and set preset positions.

Preset locations

In this page, you can set preset positions for the Network Camera. You can also select some preset positions for it to patrol. A total of 20 preset positions can be configured.

Please follow the steps below to set a preset position:

1. Adjust the shooting area to a desired position using the buttons on the right side of the window.
2. Click **Set as home** or **Default home** to define your home definition.
3. In the Preset position name text box, enter a descriptive name for the preset position. The preset position name allows up to forty characters. Click **Add** to take effect. The preset positions will show up under the Preset location list on the left-hand side.
4. To add more preset positions, please repeat step 1~3.
5. To remove a preset position from the list, select a preset position name from the Preset Positions drop-down list and then click **Delete**.
6. Click **Save** to take effect.



Video(TCP-AV) 2008/12/02 10:12:05

Pan speed: 0

Tilt speed: 0

Zoom speed: 0

Auto pan/patrol speed: 1

☐ Return to home position while idle

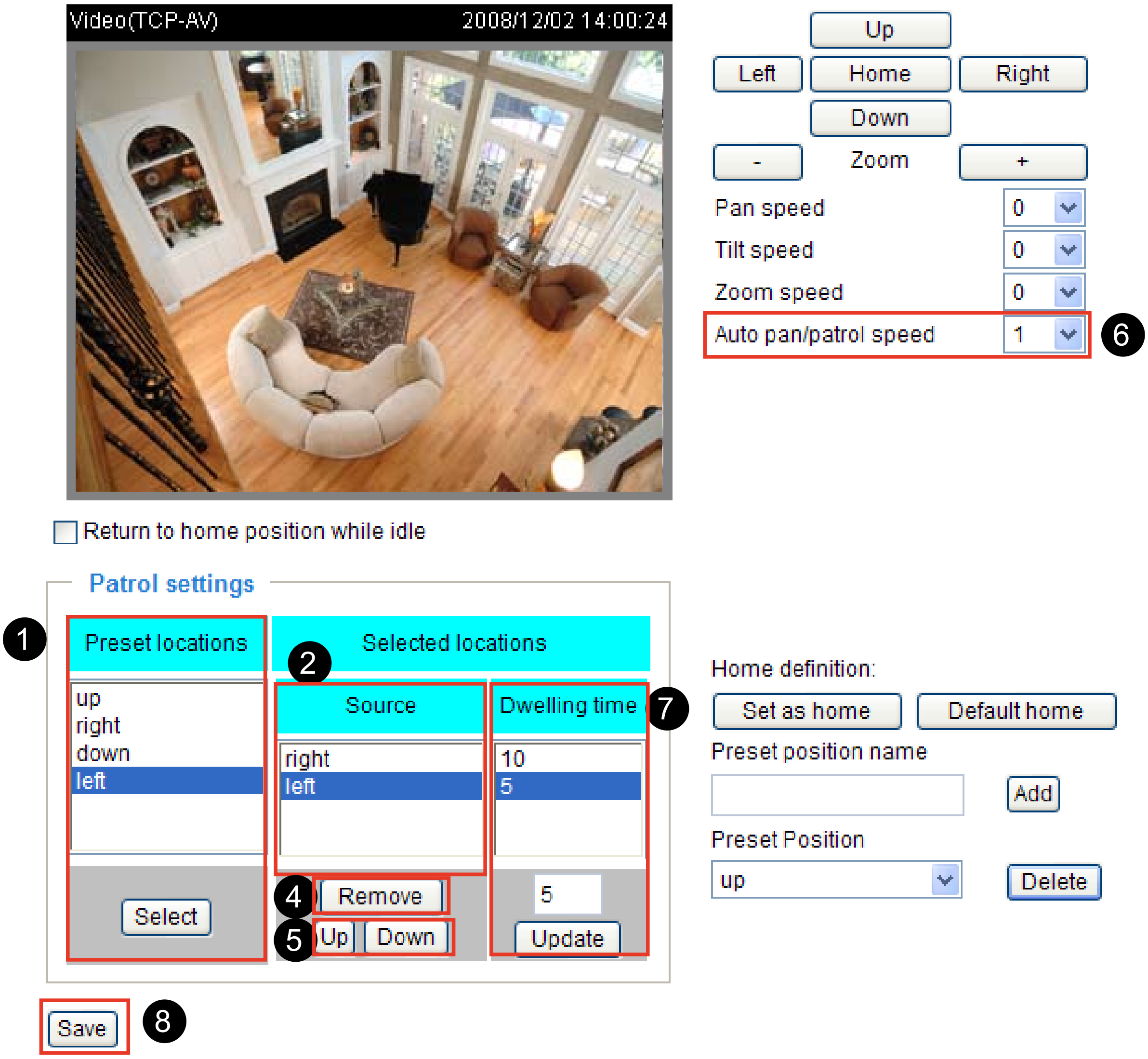
1 functions are the same as the control panel on home page

Patrol Settings

You can select some preset locations for the Network Camera to patrol.

Please follow the steps below to set a preset position:

1. Click a preset location on the list and then click **Select**.
2. The selected preset location will show up on the **Source** of **Selected locations** list.
3. Repeat step 1 and 2 to select more preset locations to patrol around.
4. If you want to delete a selected location, click it on the list and then click **Remove**.
5. Click the selected locations and then click **Up** or **Down** to arrange the order for patrolling.
6. Adjust the **Auto pan/patrol speed**. (1~5 seconds)
7. Set the **Dwelling time** for each preset location during auto patrol of the network camera. The default value is 10 seconds. You can also manually enter a value into the blank, and then click **Update**.
8. Click **Save** to enable the settings.



Pan speed 0

Tilt speed 0

Zoom speed 0

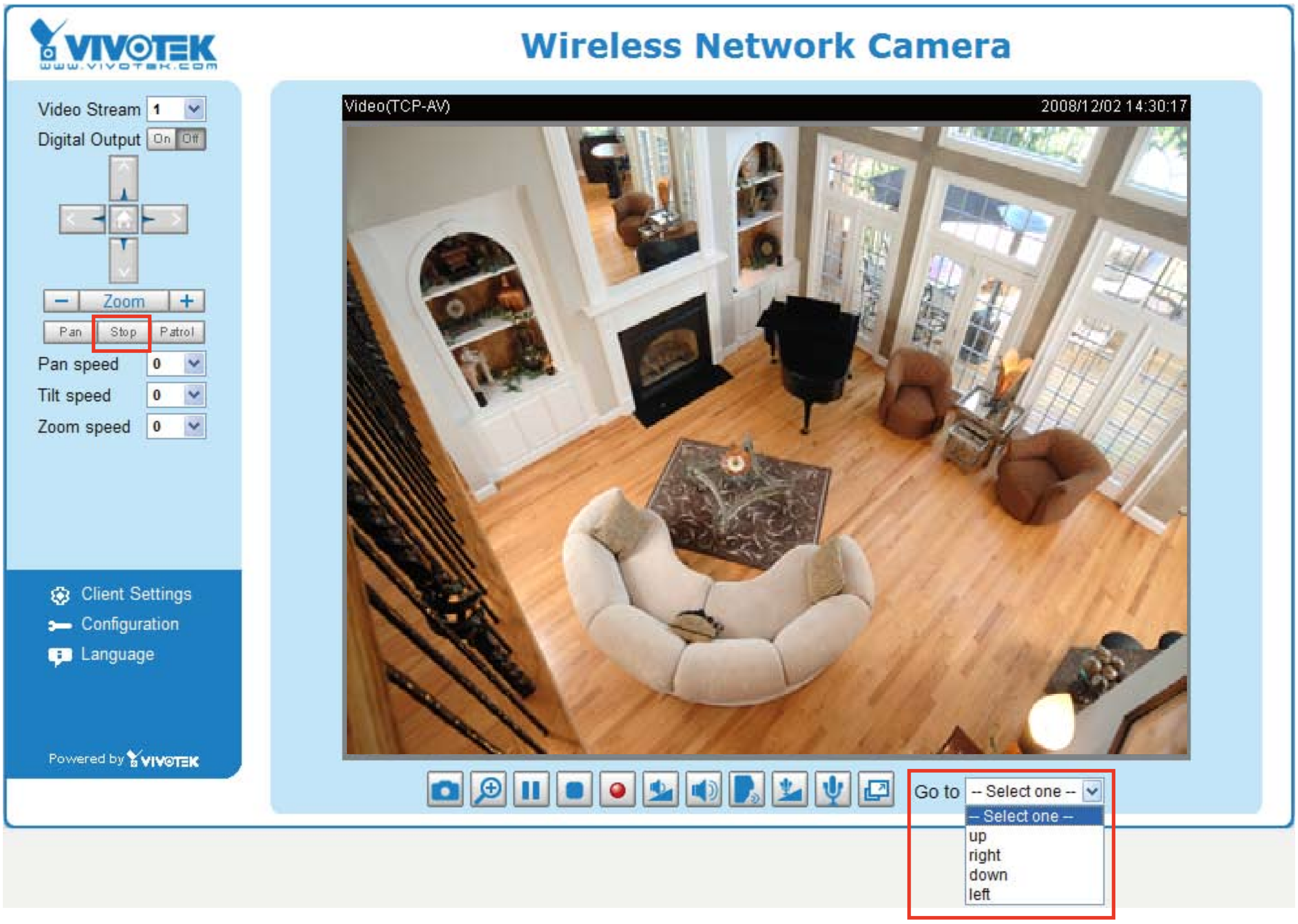
Auto pan/patrol speed 1

□ Return to home position while idle

Dwelling time: 5

Preset Position: up

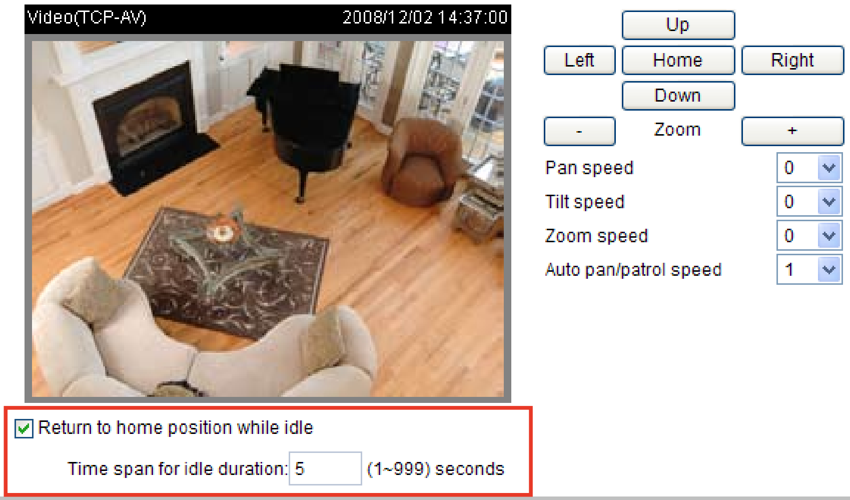
■ The preset locations will also show on the camera control panel on the Home page as below.



■ Click **Go to**: The Network Camera will move to the preset location.
■ Click **Patrol**: The Network Camera will patrol among the selected preset positions (from right to left) for once.

Return to home position while idle

If you select this option, the Network Camera will automatically pan back to the home position after idling a specific time span.
Please follow the steps below to enable this function:
1. Select **Return to home position while idle**.
2. Enter the time span for idle duration.
3. Click **Save** to enable the settings.



☑ Return to home position while idle

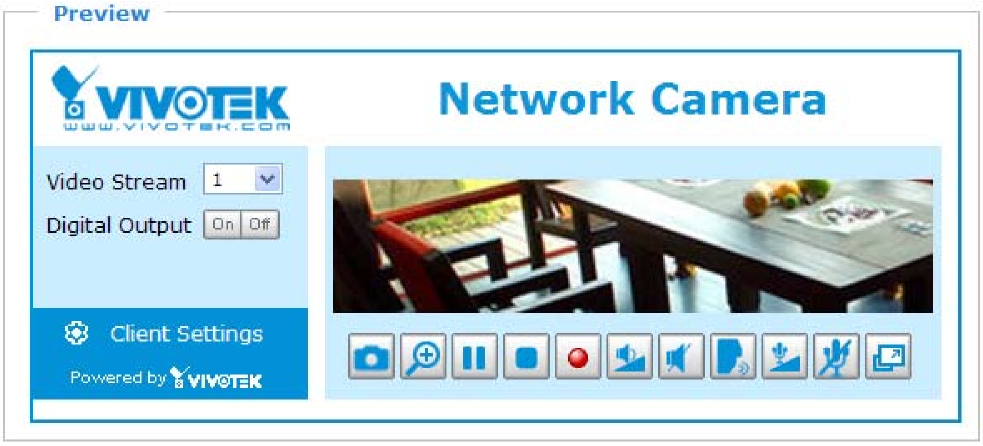
Time span for idle duration: 5 (1~999) seconds

Homepage layout Advanced mode

This section explains how to set up your own customized homepage layout.

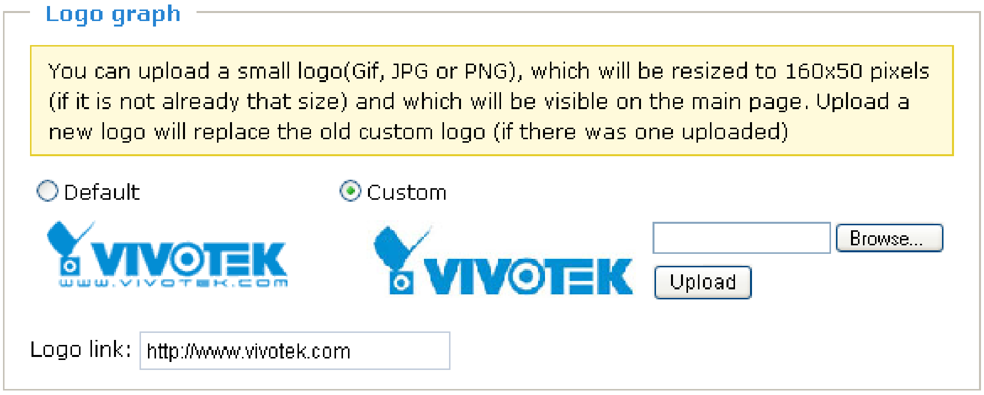
Preview

This column shows the settings of your homepage layout. You can manually setup the background and font colors in Theme Options, the third column on this page. The settings will automatically show up in this Preview column. Following shows the default setting.



Logo graph

Here you can change the logo on the top of your homepage.


Logo graph

You can upload a small logo(Gif, JPG or PNG), which will be resized to 160x50 pixels (if it is not already that size) and which will be visible on the main page. Upload a new logo will replace the old custom logo (if there was one uploaded)

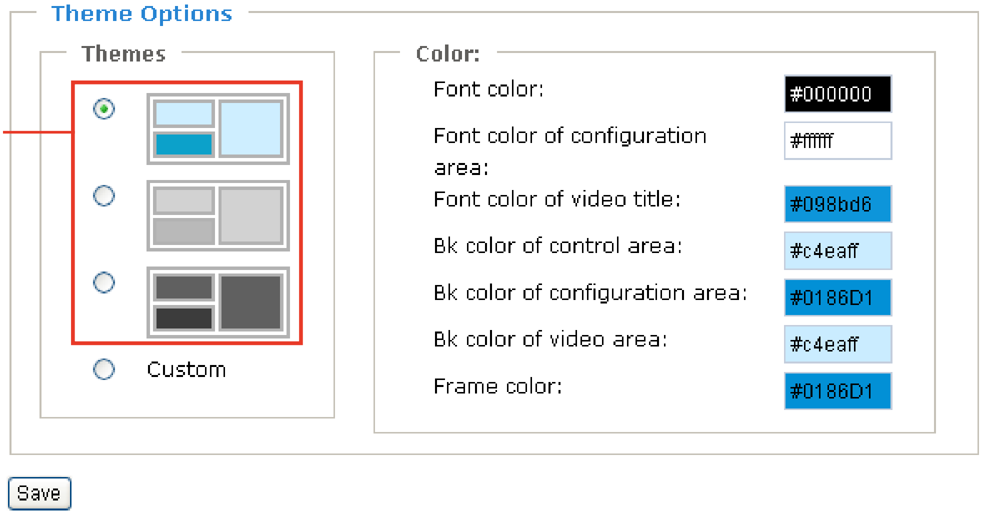
○ Default ● Custom

Logo link: http://www.vivotek.com

Follow the steps below to upload a new logo:
1. Click **Custom** to open the Browse blank.
2. Select a logo in your computer folders.
3. Click **Upload** to replace the logo with a new one.
4. Enter a website link if necessary.
5. Click **Save** to enable the settings.

Theme options

Here you can change the color of your homepage layout. There are three kinds of preset patterns for you to choose. The new layout will simultaneously present in the **Preview** column. Click **Save** to enable the settings.



preset patterns

Theme Options

Themes

●

○

○

○ Custom

Color:

Font color: #000000

Font color of configuration area: #ffffff

Font color of video title: #098bd6

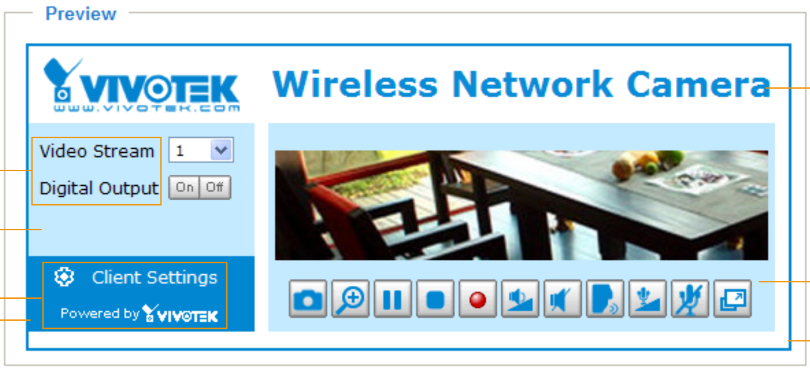
Bk color of control area: #c4eaff

Bk color of configuration area: #0186D1

Bk color of video area: #c4eaff

Frame color: #0186D1

Save



Font color of video title

Font color

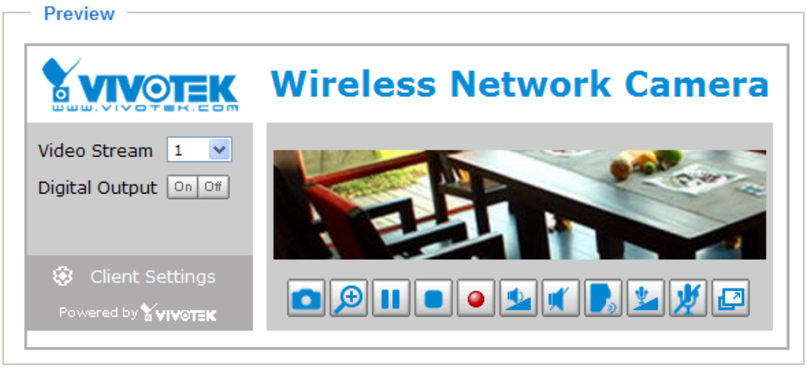
Bk color of control area

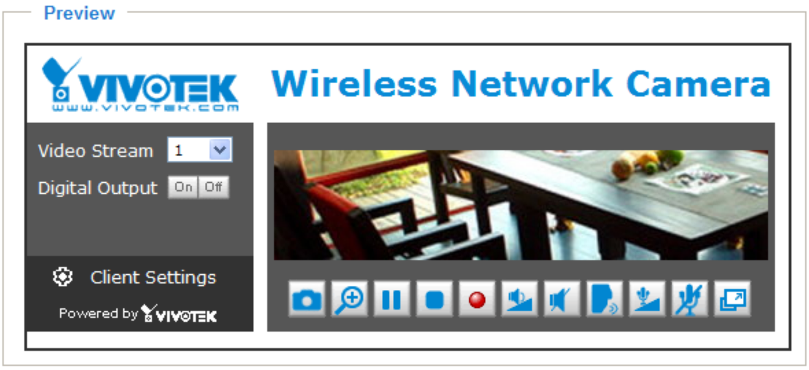
Font color of configuration area

Bk color of configuration area

Bk color of video area

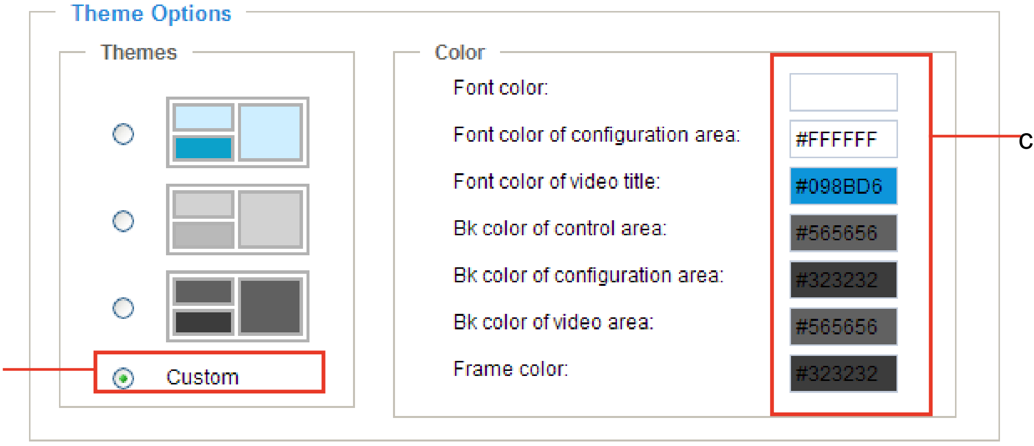
Frame color





■ Follow the steps below to set up customized homepage:

1. Click **Custom** on the left column.
2. Click a blank you want to change color on the right column.



Theme Options

Themes

○

○

○

● Custom

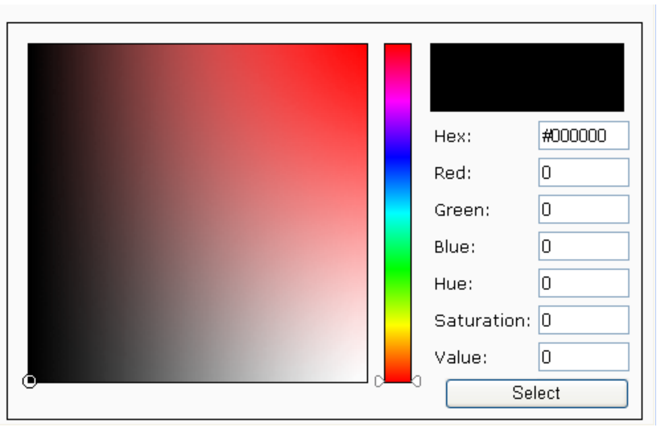
Color

Font color:	
Font color of configuration area:	#FFFFFF
Font color of video title:	#098BD6
Bk color of control area:	#565656
Bk color of configuration area:	#323232
Bk color of video area:	#565656
Frame color:	#323232

color picker

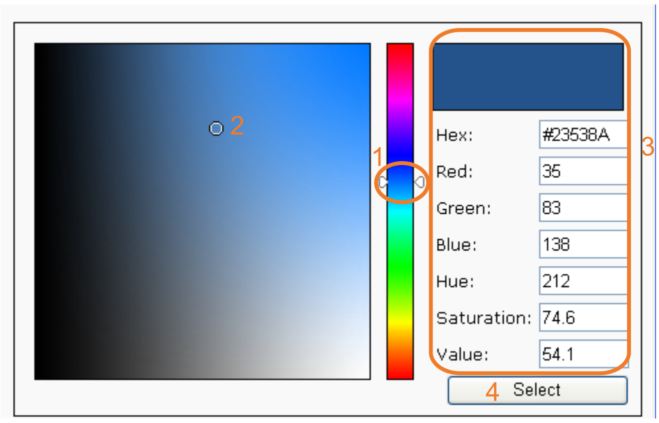
customed pattern

3. The palette window will pop up as below.



Hex:	#000000
Red:	0
Green:	0
Blue:	0
Hue:	0
Saturation:	0
Value:	0

Select



Hex:	#23538A
Red:	35
Green:	83
Blue:	138
Hue:	212
Saturation:	74.6
Value:	54.1

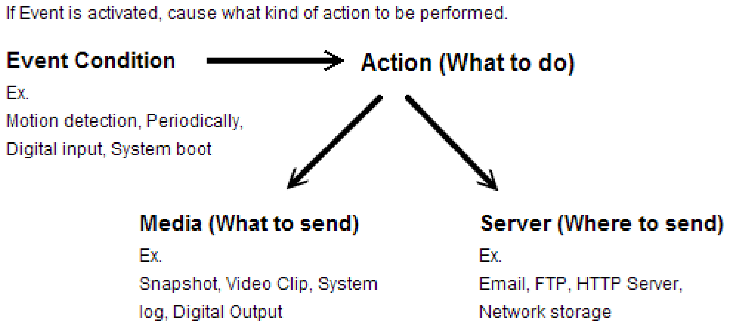
Select

4. Drag the slider bar and click on the left square to select a desired color.
5. The selected color will show up in the corresponding blank and in the **Preview** column.
6. Click **Save** to enable the settings.

Application Advanced mode

This section explains how to configure the Network Camera to react in response to particular situations (event). A typical application is that when a motion is detected, the Network Camera sends buffered images to a FTP server or e-mail address as notifications.

In the illustration, an event can be triggered by many sources, such as motion detection or external digital input devices. When an event is triggered, you can specify what kind of action will be performed. You can configure the Network Camera to send snapshots or videos to your email address or FTP site.



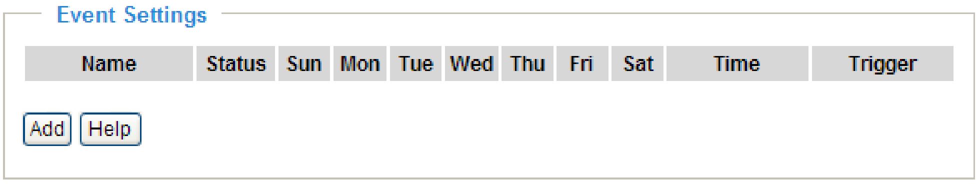
If Event is activated, cause what kind of action to be performed.

Event Condition → **Action (What to do)**

Ex.
Motion detection, Periodically,
Digital input, System boot

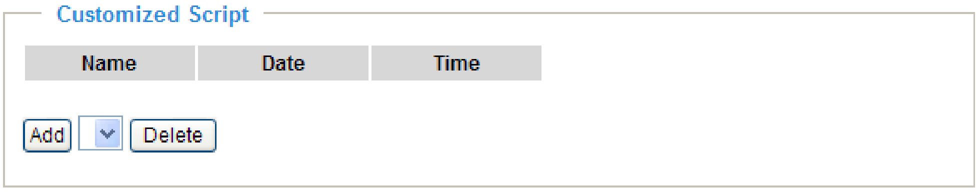
Media (What to send)
Ex.
Snapshot, Video Clip, System
log, Digital Output

Server (Where to send)
Ex.
Email, FTP, HTTP Server,
Network storage



Event Settings

Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Trigger

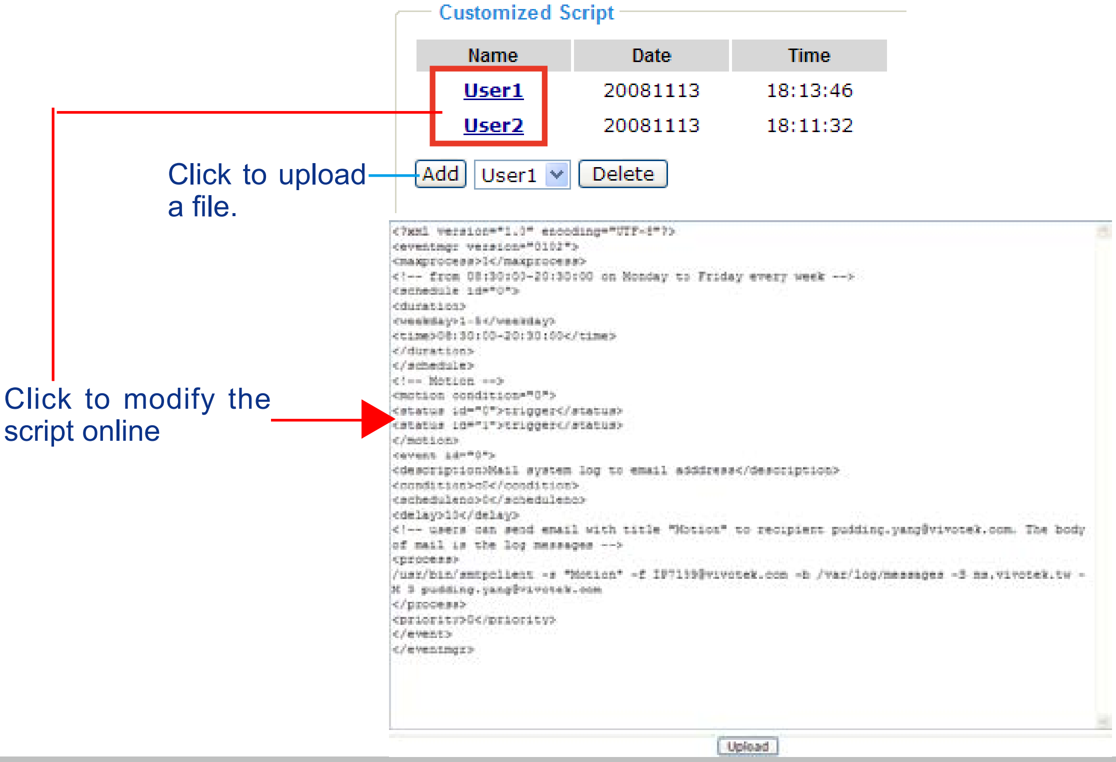


Customized Script

Name	Date	Time

Customized Script

This function is for you to upload a sample script (.xml file) to the webpage, which will save you much time on configuring the settings. Please note that there is limited number of customized scripts you can upload, if current amount of customized scripts has reached the limitation, an alert message will pop up to remind the user. If you need more information, please ask for VIVOTEK technical support.



Customized Script

Name	Date	Time
User1	20081113	18:13:46
User2	20081113	18:11:32

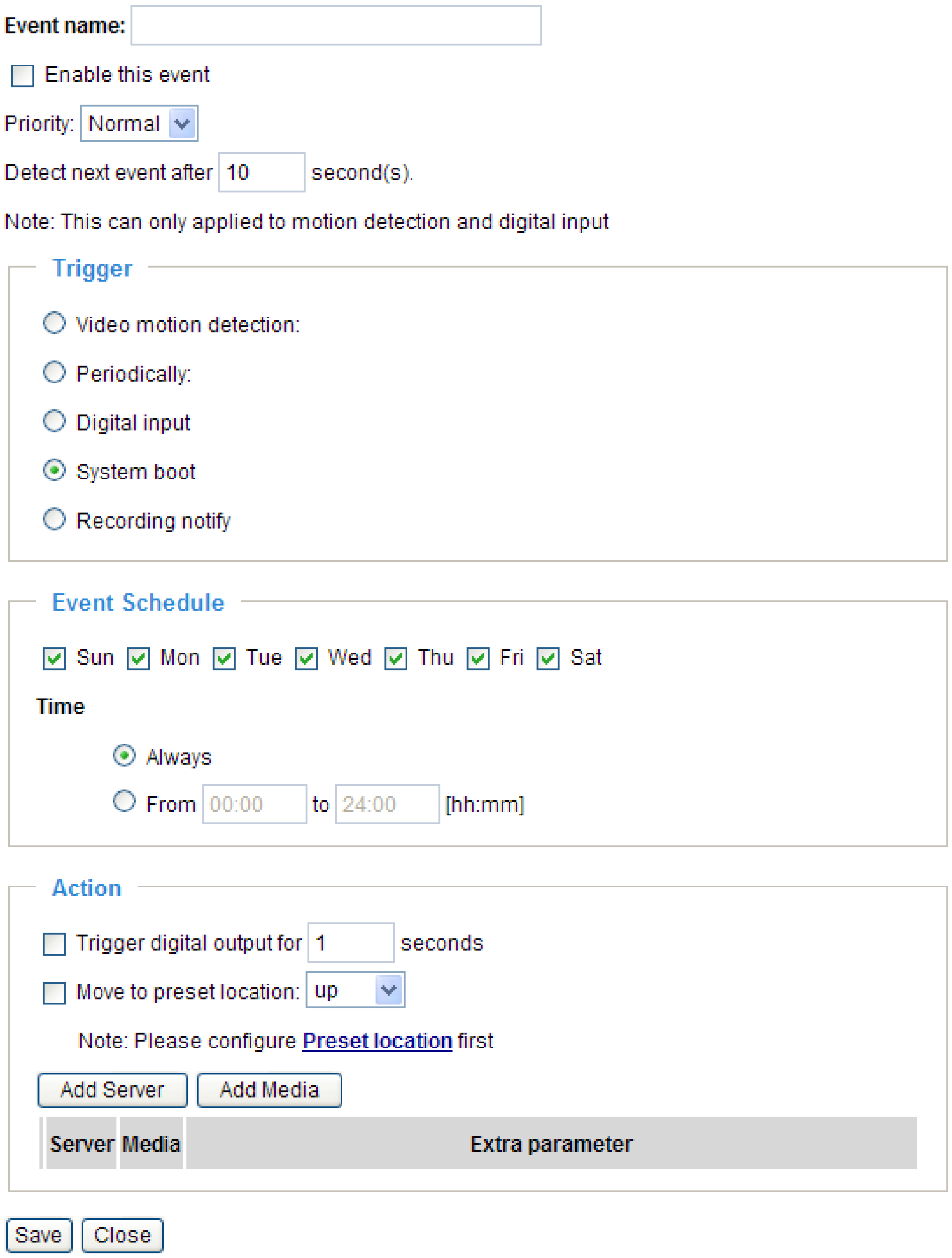
Click to upload a file.

Click to modify the script online

```
<?xml version="1.0" encoding="UTF-8"?>
<eventmgr version="0102">
<maxprocess>1</maxprocess>
<!-- from 08:30:00-20:30:00 on Monday to Friday every week -->
<schedule id="0">
<duration>
<weekday>1-5</weekday>
<time>08:30:00-20:30:00</time>
</duration>
</schedule>
<!-- Motion -->
<motion condition="0">
<status id="0">trigger</status>
<status id="1">trigger</status>
</motion>
<event id="0">
<description>Mail system log to email address</description>
<condition>c0</condition>
<scheduleno>0</scheduleno>
<delay>10</delay>
<!-- users can send email with title "Motion" to recipient pudding.yang@vivotek.com. The body
of mail is the log messages -->
<process>
/usr/bin/smtpclient -s "Motion" -f IP7139@vivotek.com -b /var/log/messages -S ms.vivotek.tw -
M 3 pudding.yang@vivotek.com
</process>
<priority>0</priority>
</event>
</eventmgr>
```

Event Settings

In the **Event Settings** column, click **Add** to open the **Event Settings** page. In this page, you can arrange three elements -- Trigger, Schedule and Action to plot an event. A total of 3 event settings can be configured.



Event name:

☐ Enable this event

Priority: Normal

Detect next event after 10 second(s).

Note: This can only applied to motion detection and digital input

Trigger

○ Video motion detection:

○ Periodically:

○ Digital input

● System boot

○ Recording notify

Event Schedule

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time

● Always

○ From 00:00 to 24:00 [hh:mm]

Action

☐ Trigger digital output for 1 seconds

☐ Move to preset location: up

Note: Please configure Preset location first

Server	Media	Extra parameter

Event name: Enter a descriptive name for the event setting.

Enable this event: Select this option to enable this event setting.

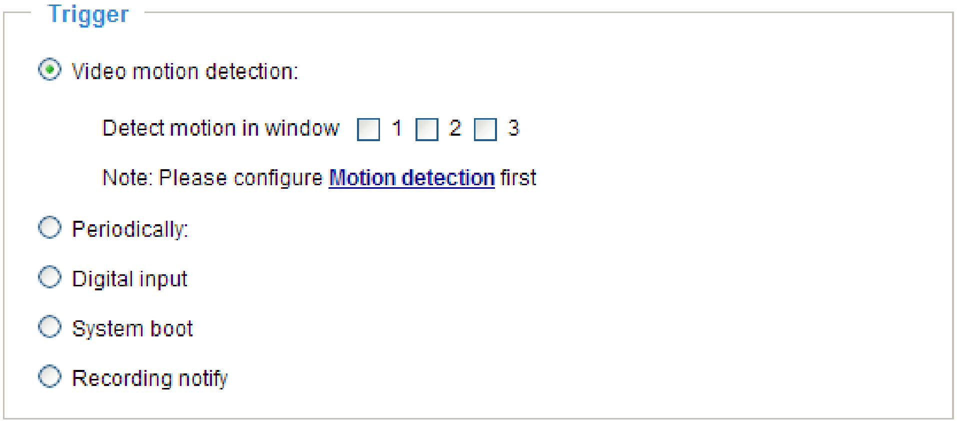
Priority: Select the relative importance of this event (High, Normal, or Low). Events with higher priority setting will be executed first.

Detect next event after ☐ seconds: Enter the duration in seconds to pause motion detection after a motion is detected.

An event is an action initiated by user-defined trigger source; it is the causal arrangement of the following three elements: Trigger, Event Schedule, and Action.

Trigger
Also referred as the cause or stimulus, defines when to trigger the Network Camera. The trigger source can be configured to use the Network Camera's built-in motion detection mechanism or external digital input devices.
There are several choices of trigger sources as below. Select the item to display the detailed configurations.

■ Video motion detection
This option makes use of the built-in motion detection mechanism as a trigger source. To enable this function, you need to configure Motion Detection window first. For more information, please refer to Motion detection on page 58 for details.



Trigger

● Video motion detection:

Detect motion in window □ 1 □ 2 □ 3

Note: Please configure Motion detection first

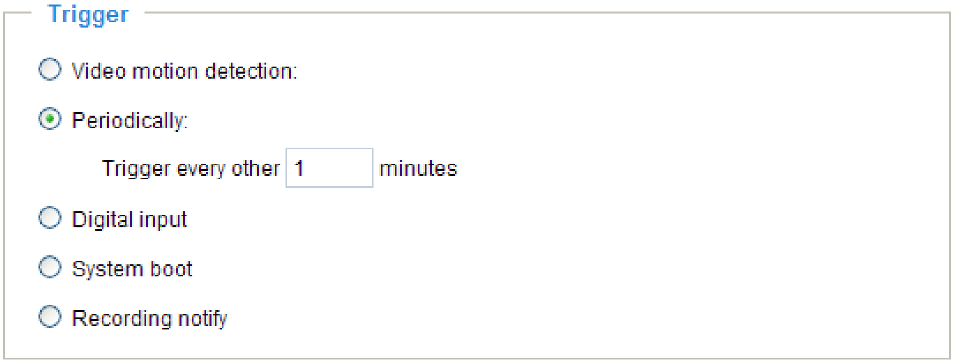
○ Periodically:

○ Digital input

○ System boot

○ Recording notify

■ Periodically
This option allows the Network Camera to trigger periodically for every other defined minute. At most 999 minutes can be set.



Trigger

○ Video motion detection:

● Periodically:

Trigger every other 1 minutes

○ Digital input

○ System boot

○ Recording notify

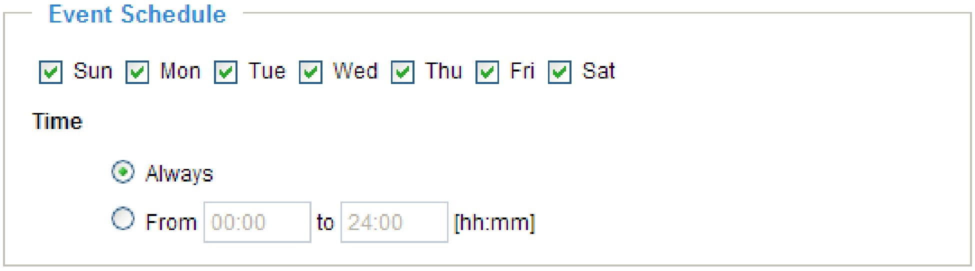
■ Digital input
This option allows the Network Camera to use external digital input device or sensor as a trigger source. Depending on your applications, there are many choices of digital input devices on the market which helps to sense any changes in temperature, vibration, sound and light, etc.

■ System boot
This option allows the Network Camera to trigger when the power of Network Camera is disconnected.

■ Recording notify
This option allows the Network Camera to trigger when the recording storage file is full or begin cycle reording. If you want receive **Recording notify message**, please refer to page 77 for detailed information.

Event Schedule

Specify the effective period for the event.



Event Schedule

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time

● Always

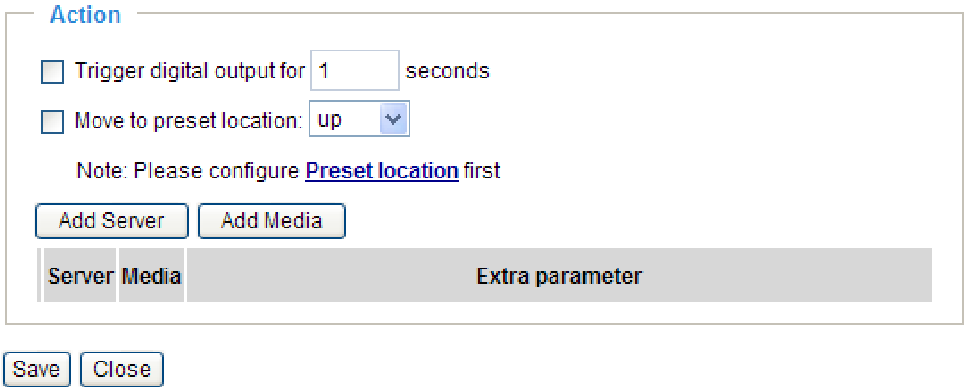
○ From 00:00 to 24:00 [hh:mm]

■ Select the days on weekly basis.

■ Select the time for recording in 24-hr time format.

Action

Define what actions to be performed by the Network Camera when a trigger is activated.



Action

□ Trigger digital output for 1 seconds

□ Move to preset location: up

Note: Please configure Preset location first

Server	Media	Extra parameter

■ Trigger digital output for □ seconds

Select this option to turn on external digital output device when a trigger is activated. Specify the length of trigger interval in the text box.

■ Move to preset location

Select this option, the Network Camera will move to the preset location when a trigger is activated. Please setup the preset locations first. Please refer to Preset locations on page 60 for detailed information.

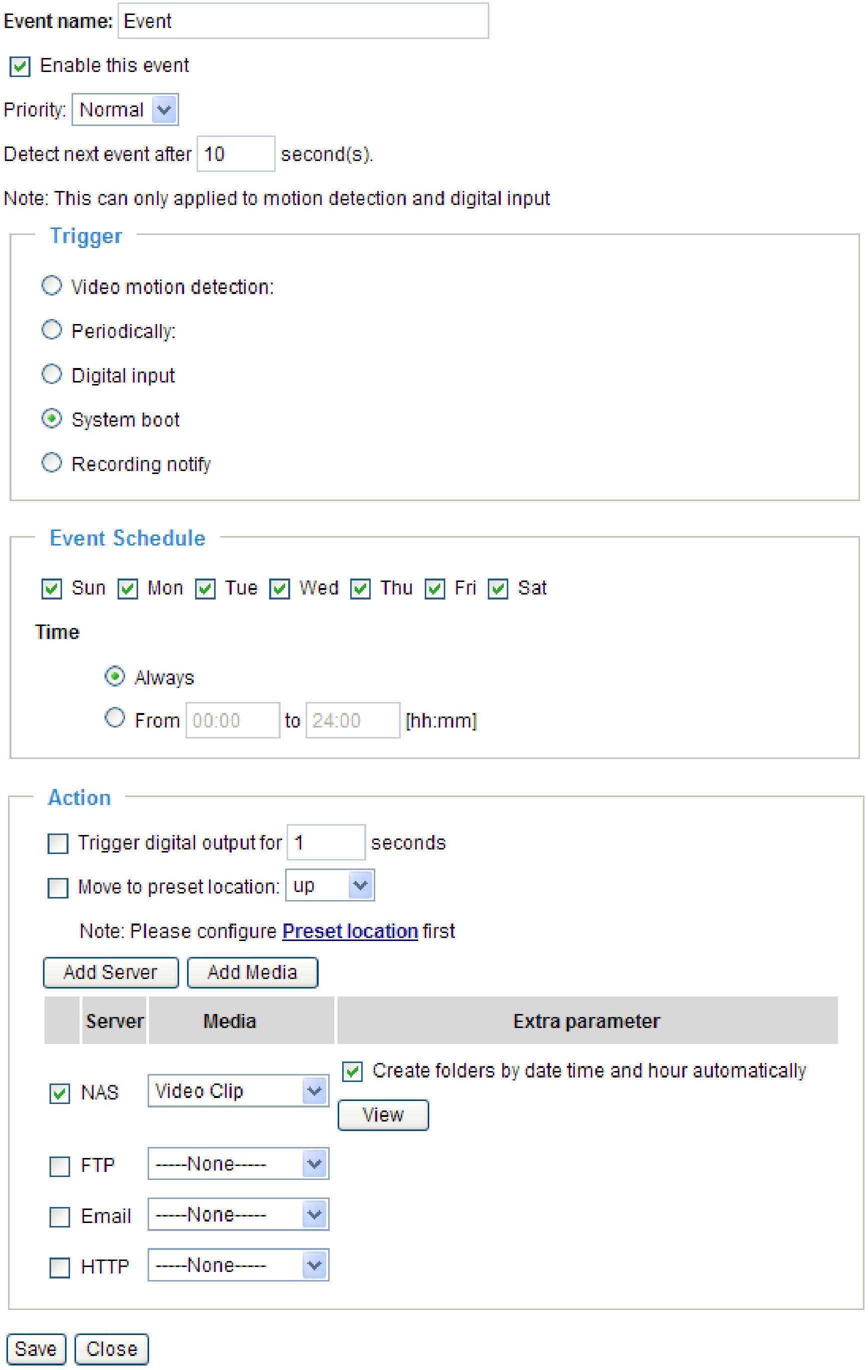
To plot an event with recorded video or snapshots, it is necessary to configure the server and media settings, so that the Network Camera will know what action shall be performed (send media files to which server) when a trigger is activated.

■ Add Server / Add Media

Click **Add Server** to configure Server Settings. For more information, please refer to Server Settings on page 72.

Click **Add Media** to configure Media Settings. For more information, please refer to Media Settings on page 75.

Here is an example of Event Settings page:



Event name: Event

☑ Enable this event

Priority: Normal

Detect next event after 10 second(s).

Note: This can only applied to motion detection and digital input

Trigger

○ Video motion detection:

○ Periodically:

○ Digital input

● System boot

○ Recording notify

Event Schedule

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time

● Always

○ From 00:00 to 24:00 [hh:mm]

Action

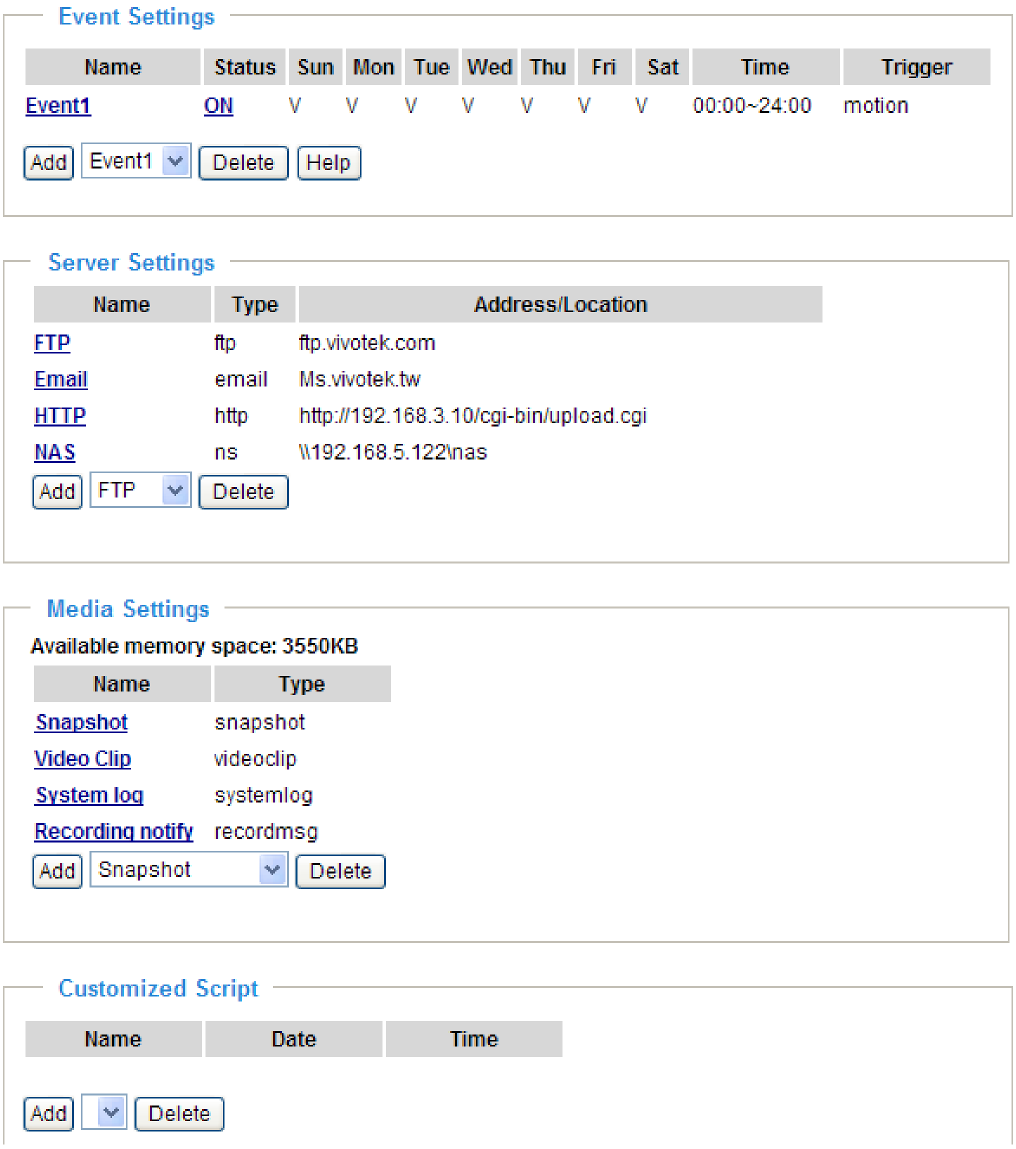
□ Trigger digital output for 1 seconds

□ Move to preset location: up

Note: Please configure Preset location first

	Server	Media	Extra parameter
☑	NAS	Video Clip	☑ Create folders by date time and hour automatically View
□	FTP	-----None-----	
□	Email	-----None-----	
□	HTTP	-----None-----	

When completed, click **Save** to take effect and then click **Close** to quit Event Settings page. The new event settings / server settings / media settings will appear in the event drop-down list on the Application page.
Here is an example of Application page with an event setting:



Event Settings

Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Trigger
Event1	ON	V	V	V	V	V	V	V	00:00~24:00	motion

Server Settings

Name	Type	Address/Location
FTP	ftp	ftp.vivotek.com
Email	email	Ms.vivotek.tw
HTTP	http	http://192.168.3.10/cgi-bin/upload.cgi
NAS	ns	\\192.168.5.122\nas

Media Settings

Available memory space: 3550KB

Name	Type
Snapshot	snapshot
Video Clip	videoclip
System log	systemlog
Recording notify	recordmsg

Customized Script

Name	Date	Time

When the Event Status is **ON**, once an event is triggered by motion detection, the Network Camera will automatically send snapshots via e-mail.

If you want to stop the event trigger, you can click **ON** to turn it into **OFF** status or click **Delete** to remove the event setting.

To remove a server setting from the list, select a server name from the drop-down list and then click **Delete**. Note that only when the server setting is not being applied to an event setting can it be deleted.

To remove a media setting from the list, select a media name from the drop-down list and then click **Delete**. Note that only when the media setting is not being applied to an event setting can it be deleted.

Server Settings

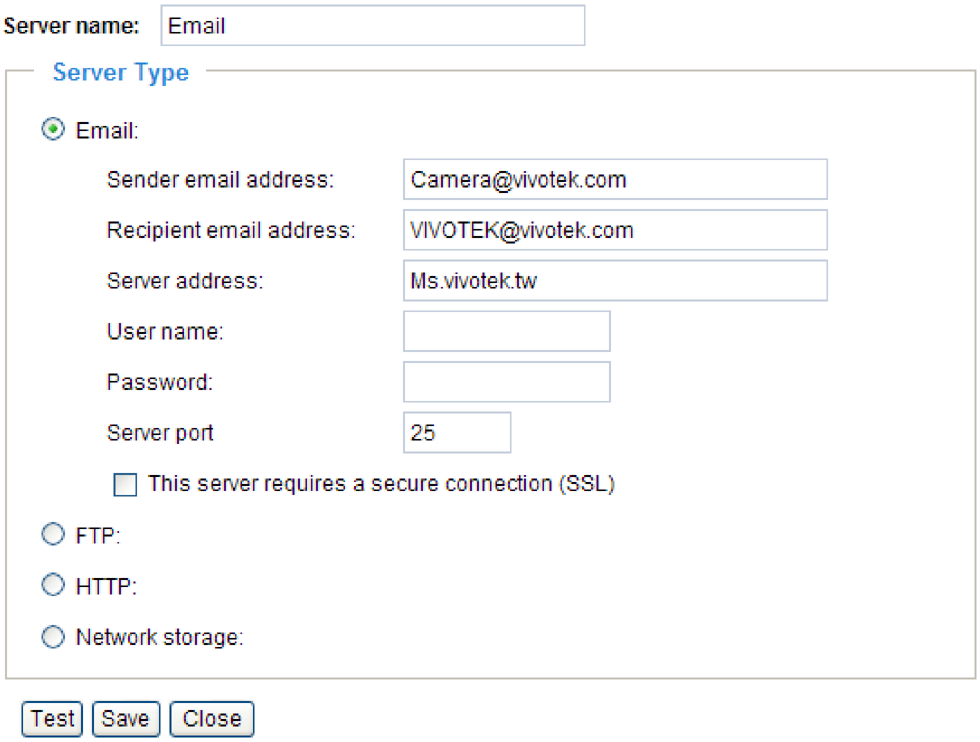
Click **Add Server** on Event Settings page to open the server setting page. In this page, you can specify where the notification messages will be send when a trigger is activated. A total of 5 server settings can be configured.

Server name: Enter a descriptive name for the server setting.

Server Type

There are four choices of server types available: Email, FTP, HTTP, and Network storage. Select the item to display the detailed configurations. You can configure either one or all of them.

Email: Select to send the media files via Email when a trigger is activated.



Server name: Email

Server Type

● Email:

Sender email address: Camera@vivotek.com

Recipient email address: VIVOTEK@vivotek.com

Server address: Ms.vivotek.tw

User name:

Password:

Server port 25

□ This server requires a secure connection (SSL)

○ FTP:

○ HTTP:

○ Network storage:

■ Sender email address: Enter the email address of the sender.

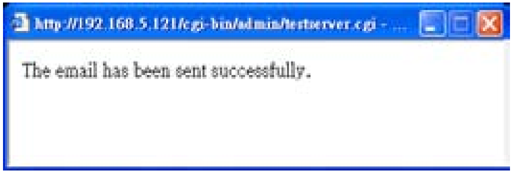
■ Recipient email address: Enter the email address of the recipient.

■ Server address: Enter the domain name or IP address of the email server.

■ User name: Enter the user name of the email account if necessary.

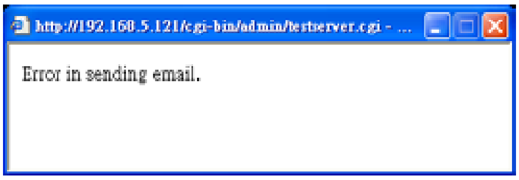
■ Password: Enter the password of the email account if necessary.

To verify if the email settings are correctly configured, click **Test**. The result will be shown in a pop-up window. If it works, you will also receive an email indicating the result. Click **Save** to enable the settings, and then click **Close** to quit the page.



http://192.168.5.121/cgi-bin/admin/testserver.cgi - ...

The email has been sent successfully.



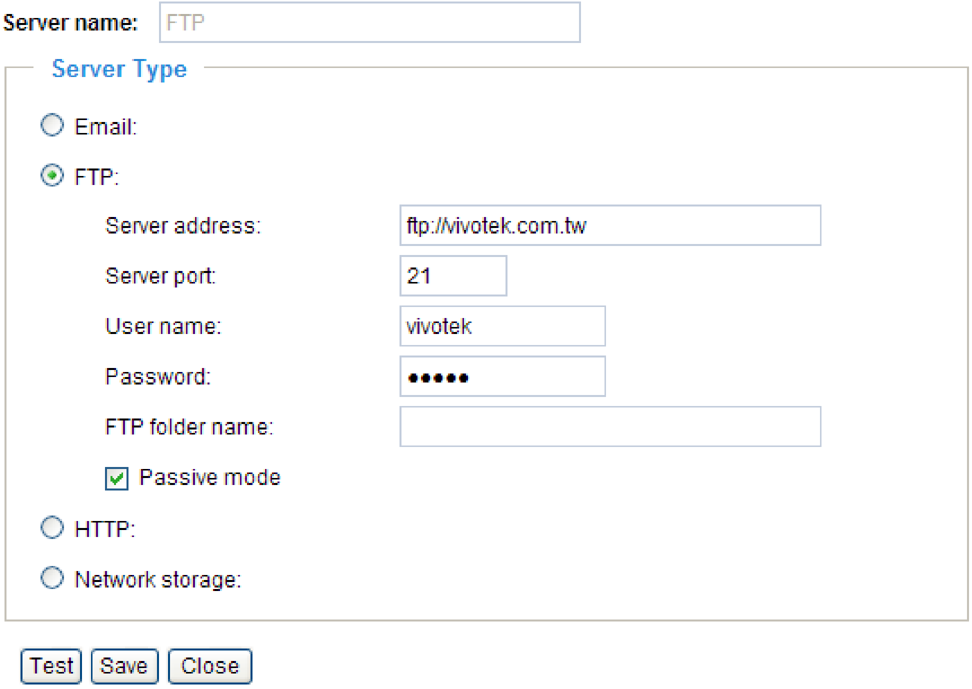
http://192.168.5.121/cgi-bin/admin/testserver.cgi - ...

Error in sending email.

If your SMTP server requires a secure connection (SSL), check **This server requires a secure connection (SSL).**

Click **Save** to enable the settings, and then click **Close** to quit the page.

FTP: Select to send the media files to a FTP server when a trigger is activated.



Server name: FTP

Server Type

○ Email:

● FTP:

Server address: ftp://vivotek.com.tw

Server port: 21

User name: vivotek

Password: •••••

FTP folder name:

☑ Passive mode

○ HTTP:

○ Network storage:

■ Server address: Enter the domain name or IP address of the FTP server.

■ Server port
By default, the FTP port server is set to 21. Also, it can be assigned with another port number between 1025 and 65535.

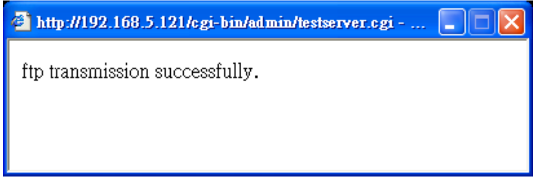
■ User name: Enter the login name of the FTP account.

■ Password: Enter the password of the FTP account.

■ Remote folder name
Enter a folder to place the media file. If the folder name does not exist, the Network Camera will create one on the FTP server.

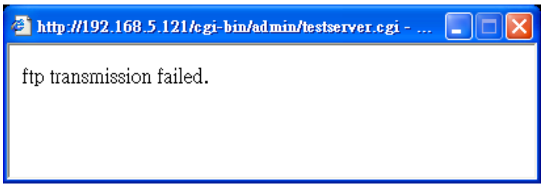
■ Passive Mode
Most firewalls do not accept new connections initiated from external requests. If the FTP server supports passive mode, select this option to enable passive mode FTP and allow data transmission to pass through the firewall.

To verify if the FTP settings are correctly configured, click **Test**. The result will be shown in a pop-up window as below. If it works, you will also receive a test.txt file on the FTP server.



http://192.168.5.121/cgi-bin/admin/testserver.cgi - ...

ftp transmission successfully.

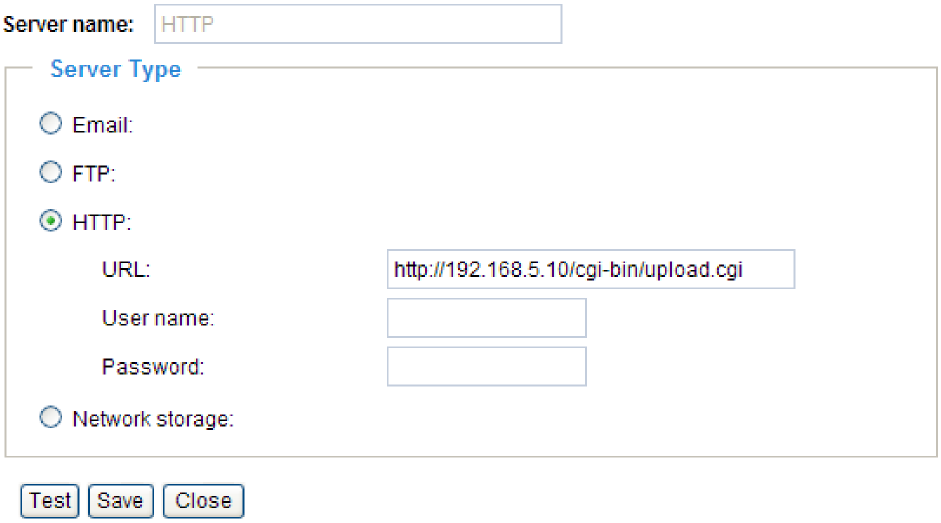


http://192.168.5.121/cgi-bin/admin/testserver.cgi - ...

ftp transmission failed.

Click **Save** to enable the settings, and then click **Close** to quit the page.

HTTP: Select to send the media files to a HTTP server when a trigger is activated.



Server name: HTTP

Server Type

○ Email:

○ FTP:

● HTTP:

URL: http://192.168.5.10/cgi-bin/upload.cgi

User name:

Password:

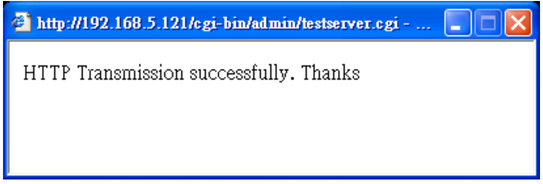
○ Network storage:

■ URL: Enter the URL of the HTTP server.

■ User name: Enter the user name if necessary.

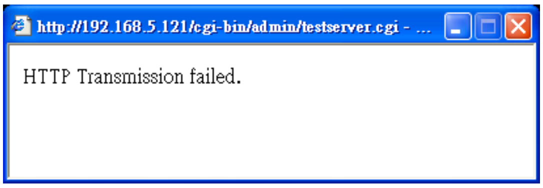
■ Password: Enter the password if necessary.

To verify if the HTTP settings are correctly configured, click **Test**. The result will be shown in a pop-up window as below. If it works, you will also receive a test.txt file on the HTTP server.



http://192.168.5.121/cgi-bin/admin/testserver.cgi - ...

HTTP Transmission successfully. Thanks



http://192.168.5.121/cgi-bin/admin/testserver.cgi - ...

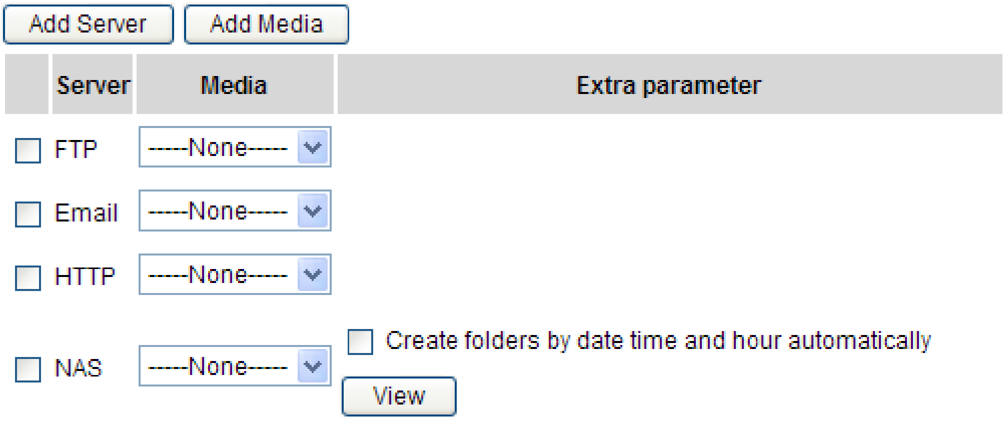
HTTP Transmission failed.

Click **Save** to enable the settings, and then click **Close** to quit the page.

Network storage: Select to send the media files to a network storage when a trigger is activated. Please refer to **Network Storage Setting** on page 79 for details.

Click **Save** to enable the settings, and then click **Close** to quit the page.

When completed, the new server settings will automatically show up on the Event Settings page.
For example:



	Server	Media	Extra parameter
□	FTP	-----None-----	
□	Email	-----None-----	
□	HTTP	-----None-----	
□	NAS	-----None-----	□ Create folders by date time and hour automatically

Media Settings

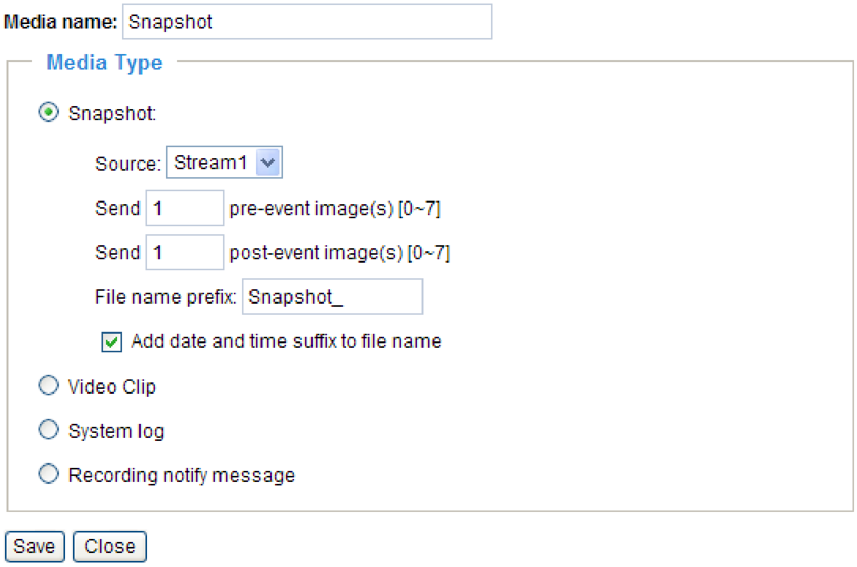
Click **Add Media** on Event Settings page to open the media settings page. In this page, you can specify what kind of media to send when a trigger is activated. A total of 5 media settings can be configured.

Media name: Enter a descriptive name for the media setting.

Media Type

There are three choices of media types available: Snapshot, Video clip, and System log. Select the item to display the detailed configurations. You can configure either one or all of them.

Snapshot: Select to send snapshots when a trigger is activated.



Media name: Snapshot

Media Type

● Snapshot:

Source: Stream1

Send 1 pre-event image(s) [0~7]

Send 1 post-event image(s) [0~7]

File name prefix: Snapshot_

☑ Add date and time suffix to file name

○ Video Clip

○ System log

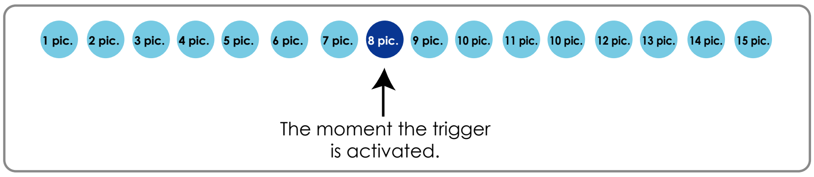
○ Recording notify message

■ Source: Select to take snapshots from stream 1 or stream 2.

■ Send □ pre-event images
The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Enter a number to decide how many images to be captured before a trigger is activated. Up to 7 images can be generated.

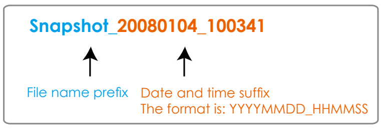
■ Send □ post-event images
Enter a number to decide how many images to be captured after a trigger is activated. Up to 7 images can be generated.

For example, if both the Send pre-event images and Send post-event images are set to 7, a total of 15 images are generated after a trigger is activated.



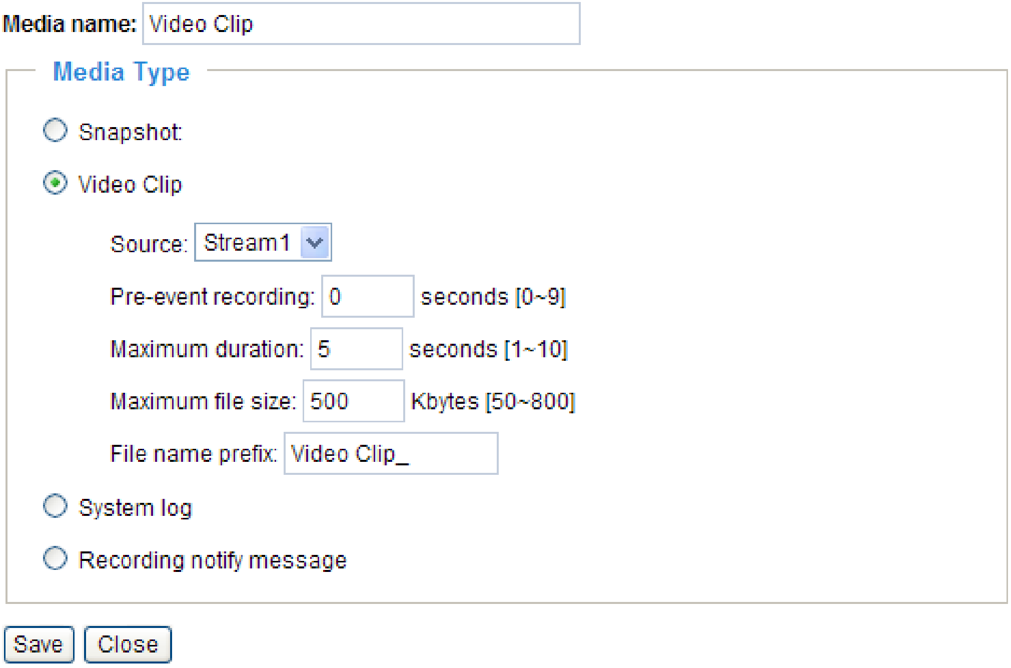
■ File Name Prefix
Enter the text that will be put in front of the file name.

■ Add date and time suffix to the file name
Select this option to add date and time to the file name suffix.
For example:



Click **Save** to enable the settings, and then click **Close** to quit the page.

Video clip: Select to send video clips when a trigger is activated.



Media name: Video Clip

Media Type

○ Snapshot

● Video Clip

Source: Stream1

Pre-event recording: 0 seconds [0~9]

Maximum duration: 5 seconds [1~10]

Maximum file size: 500 Kbytes [50~800]

File name prefix: Video Clip_

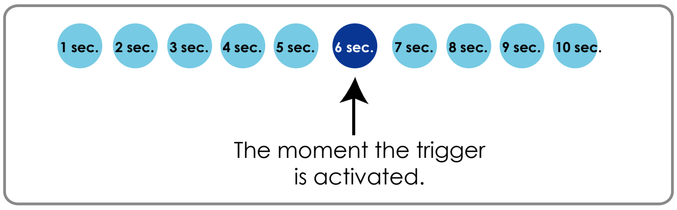
○ System log

○ Recording notify message

■ Source: Select to record video clips from stream 1 or stream 2.

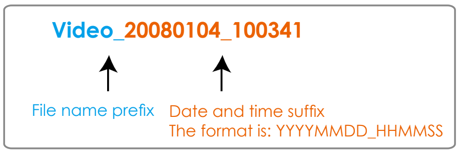
■ Pre-event recording
The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Enter a number to decide how many seconds for video clips recording before a trigger is activated. Up to 9 seconds can be set.

■ Maximum duration
Specify the maximal recording duration in seconds. Up to 10 seconds can be set.
For example, if the Pre-event recording is set to five seconds and the Maximum duration is set to ten seconds, the Network Camera continues to record for another 4 seconds after a trigger is activated.



■ Maximum file size
Specify the maximal file size allowed.

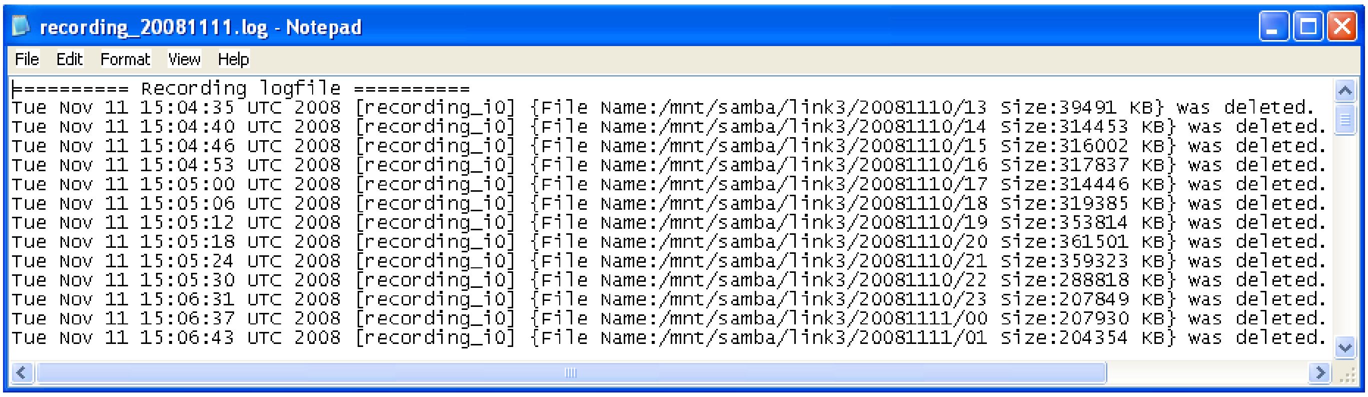
■ File Name Prefix
Enter the text that will be put in front of the file name.
For example:



Click **Save** to enable the settings, and then click **Close** to quit the page.

System log: Select to send a system log when a trigger is activated.
Click **Save** to enable the settings, and then click **Close** to quit the page.

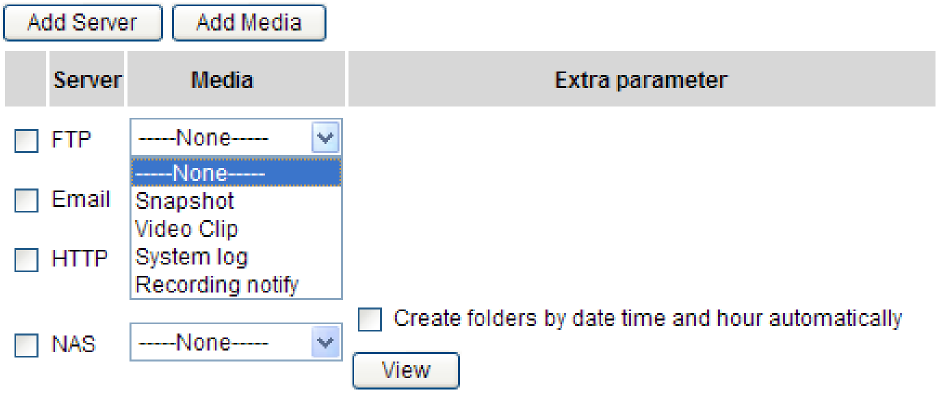
Recording notify message: Select to send a recording notify message when a trigger is activated. Following is an example of recording notify message (.txt file), which shows a list of deleted recorded data due to cycle recording.



```
========== Recording logfile ==========
Tue Nov 11 15:04:35 UTC 2008 [recording_i0] {File Name:/mnt/samba/link3/20081110/13 Size:39491 KB} was deleted.
Tue Nov 11 15:04:40 UTC 2008 [recording_i0] {File Name:/mnt/samba/link3/20081110/14 Size:314453 KB} was deleted.
Tue Nov 11 15:04:46 UTC 2008 [recording_i0] {File Name:/mnt/samba/link3/20081110/15 Size:316002 KB} was deleted.
Tue Nov 11 15:04:53 UTC 2008 [recording_i0] {File Name:/mnt/samba/link3/20081110/16 Size:317837 KB} was deleted.
Tue Nov 11 15:05:00 UTC 2008 [recording_i0] {File Name:/mnt/samba/link3/20081110/17 Size:314446 KB} was deleted.
Tue Nov 11 15:05:06 UTC 2008 [recording_i0] {File Name:/mnt/samba/link3/20081110/18 Size:319385 KB} was deleted.
Tue Nov 11 15:05:12 UTC 2008 [recording_i0] {File Name:/mnt/samba/link3/20081110/19 Size:353814 KB} was deleted.
Tue Nov 11 15:05:18 UTC 2008 [recording_i0] {File Name:/mnt/samba/link3/20081110/20 Size:361501 KB} was deleted.
Tue Nov 11 15:05:24 UTC 2008 [recording_i0] {File Name:/mnt/samba/link3/20081110/21 Size:359323 KB} was deleted.
Tue Nov 11 15:05:30 UTC 2008 [recording_i0] {File Name:/mnt/samba/link3/20081110/22 Size:288818 KB} was deleted.
Tue Nov 11 15:06:31 UTC 2008 [recording_i0] {File Name:/mnt/samba/link3/20081110/23 Size:207849 KB} was deleted.
Tue Nov 11 15:06:37 UTC 2008 [recording_i0] {File Name:/mnt/samba/link3/20081111/00 Size:207930 KB} was deleted.
Tue Nov 11 15:06:43 UTC 2008 [recording_i0] {File Name:/mnt/samba/link3/20081111/01 Size:204354 KB} was deleted.
```

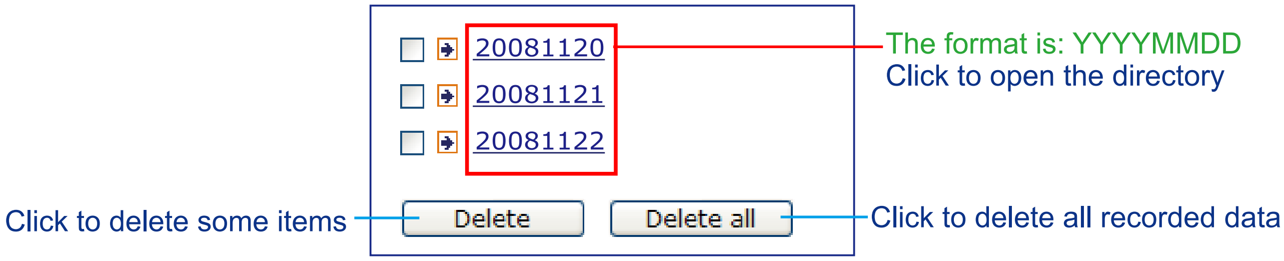
When completed, click **Save** to take effect, and then click **Close** to quit this page. The new media settings will show up on the Event Settings page.

Then you can continue to select a server and media type for the event. Please go back to page 70 for detailed information.



■ Create folders by date time and hour automatically: If you check this item, the system will generate folders automatically by date.

■ View: Click this button to open a file list window. This function is only for SD card and Network Storage. Following is an example of file destination with video clips:



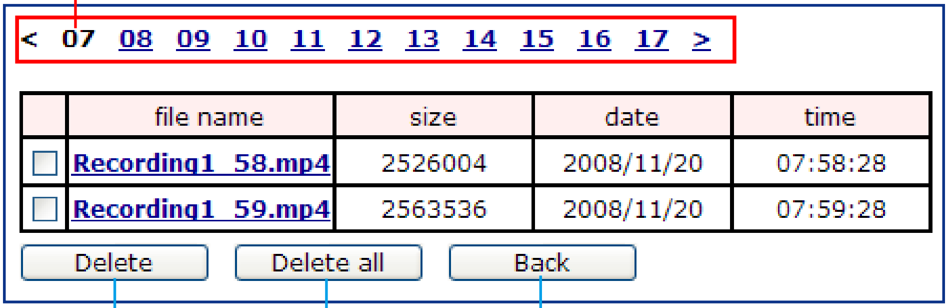
The format is: YYYYMMDD
Click to open the directory

Click to delete some items

Click to delete all recorded data

Click 20081120 to open the directory:

The format is: HH (24r)
Click to open the file list of that hour



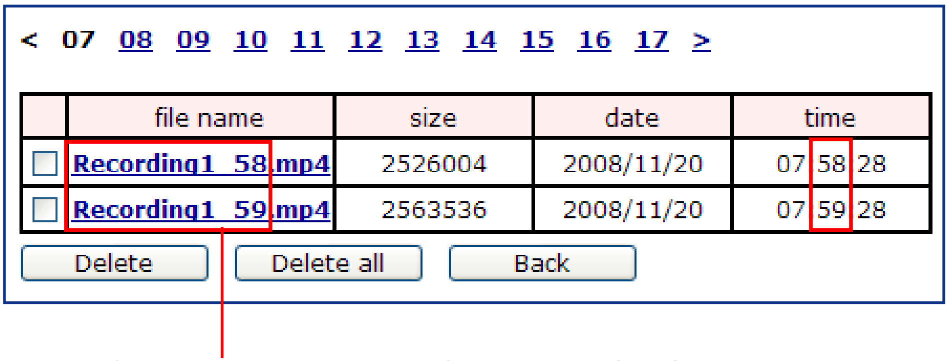
< 07 08 09 10 11 12 13 14 15 16 17 >

	file name	size	date	time
□	Recording1_58.mp4	2526004	2008/11/20	07:58:28
□	Recording1_59.mp4	2563536	2008/11/20	07:59:28

Click to delete some items

Click to do back to upper layer of the directory

Click to delete all recorded data



< 07 08 09 10 11 12 13 14 15 16 17 >

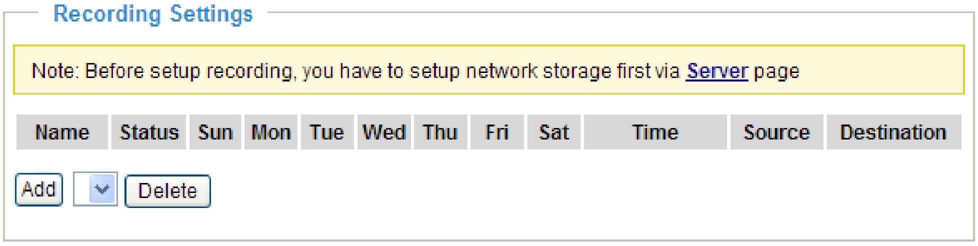
	file name	size	date	time
□	Recording1_58.mp4	2526004	2008/11/20	07:58:28
□	Recording1_59.mp4	2563536	2008/11/20	07:59:28

The format is: File name prefix + Minute (mm)
You can set up the File name prefix on Media Settings page.
Please refer to page 75 for detailed information.

Recording Advanced mode

This section explains how to configure the recording settings for the Network Camera.

Recording Settings



Recording Settings

Note: Before setup recording, you have to setup network storage first via Server page

Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Source	Destination

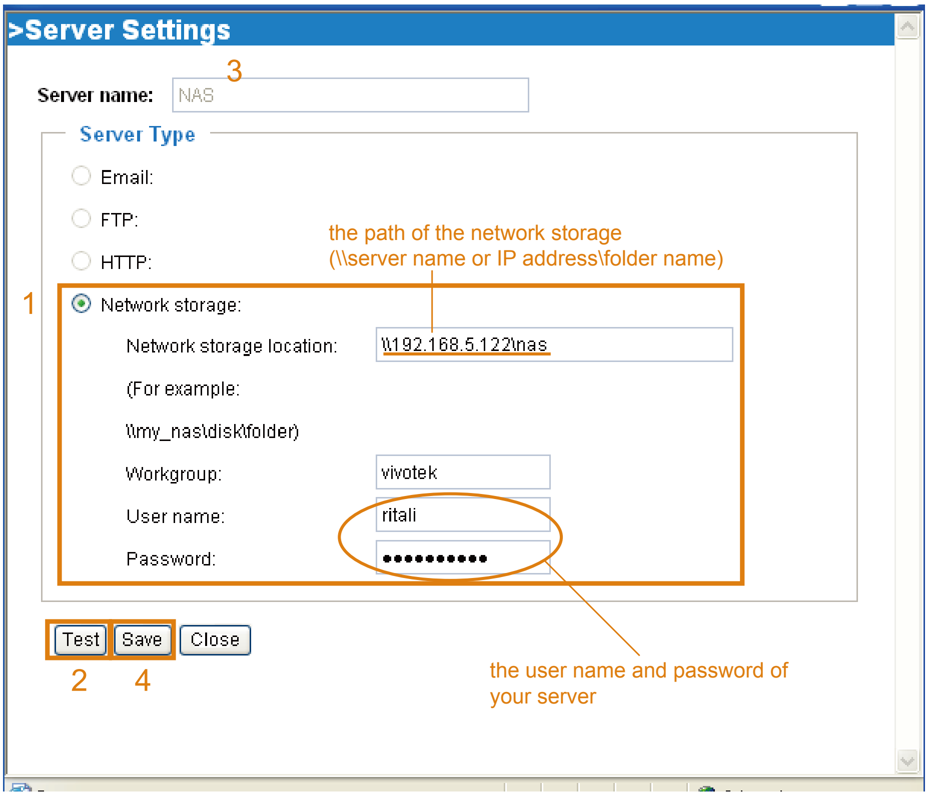
NOTE

► *Before setting up this page, please set up the Network Storage on the Server Settings page first.*

Network Storage Setting

Click Server to open the Server Settings page and follow the steps below to set up:

1. Fill in the information of your server.
   For example:



>Server Settings

Server name: NAS

Server Type

○ Email:

○ FTP:

○ HTTP:

● Network storage:

Network storage location: \\192.168.5.122\nas

(For example:

\\my_nas\disk\folder)

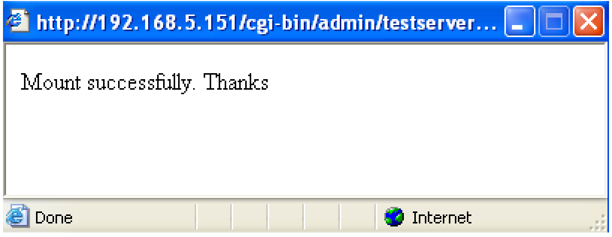
Workgroup: vivotek

User name: ritali

Password: ●●●●●●●●●●●

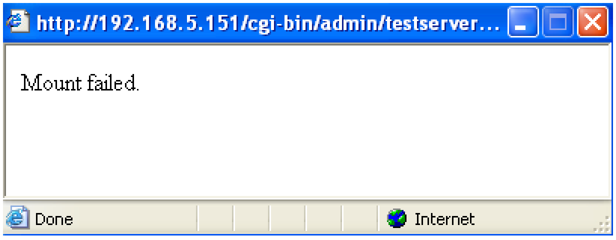
3
1
the path of the network storage
(\\server name or IP address\folder name)
Test
Save
Close
2
4
the user name and password of
your server

2. Click **Test** to check the setting. The result will be shown in a pop-up window.



http://192.168.5.151/cgi-bin/admin/testserver...

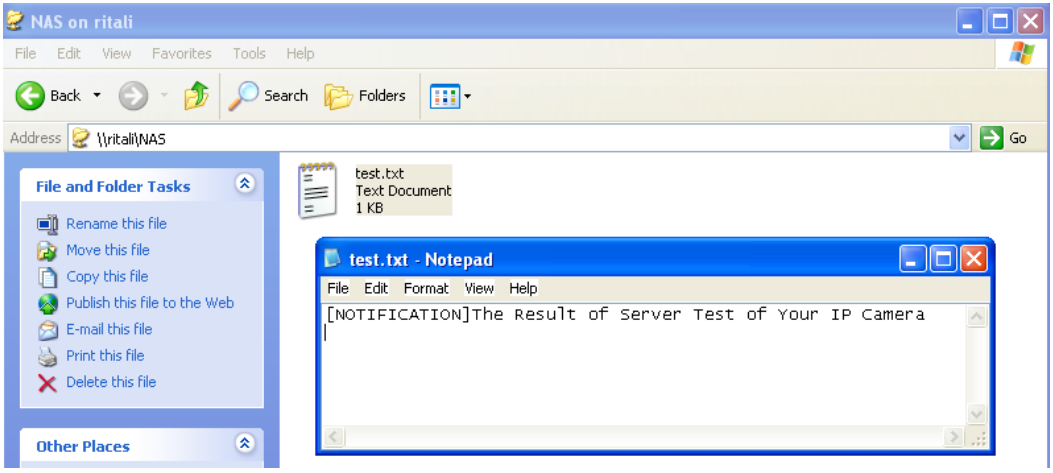
Mount successfully. Thanks



http://192.168.5.151/cgi-bin/admin/testserver...

Mount failed.

If it works, you will also receive a test.txt file on the network storage server.

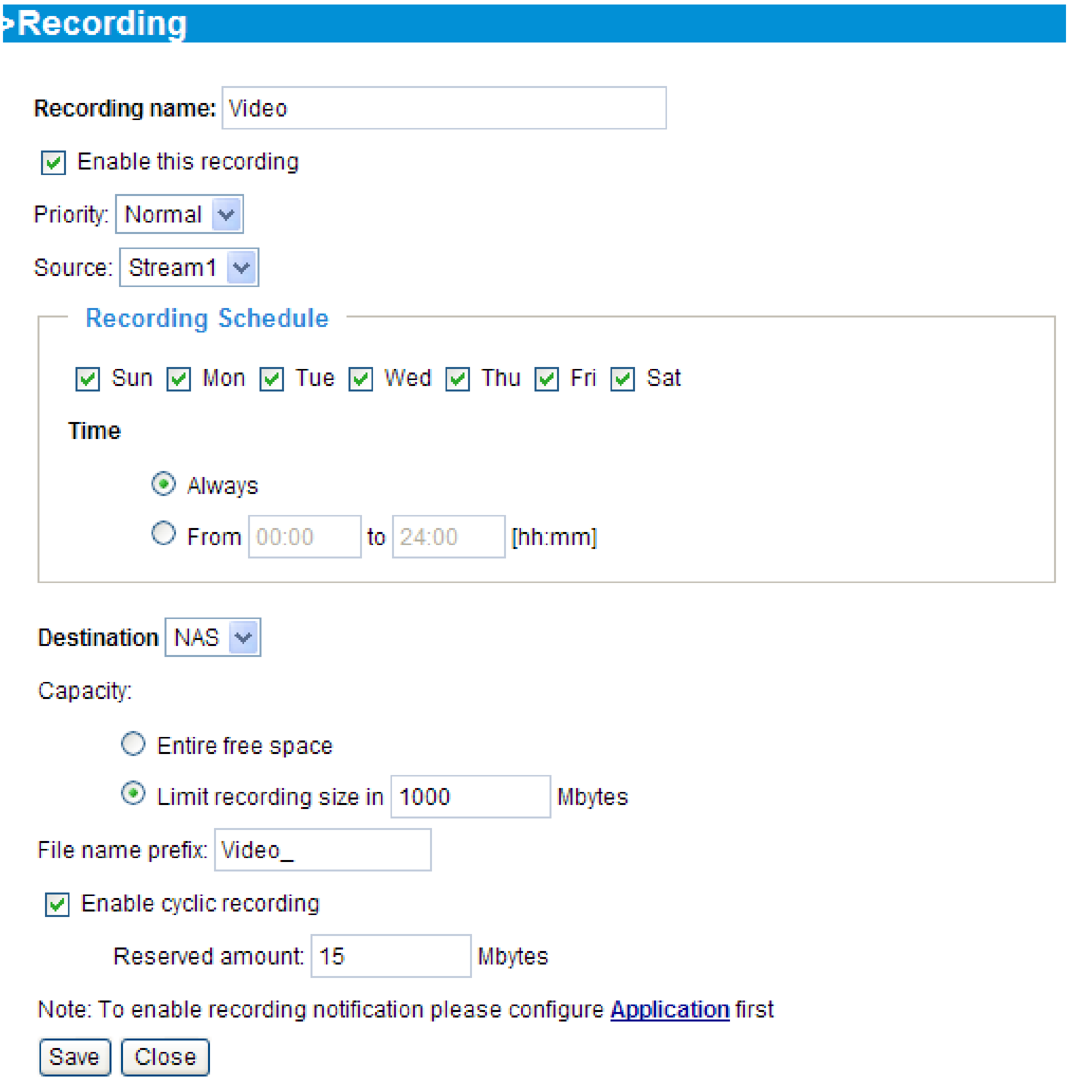


```
[NOTIFICATION]The Result of Server Test of Your IP Camera
```

3. Enter a descriptive server name.
4. Click **Save** to finish the setting and click **Close** to quit the page.

Recording Settings

Click **Add** to open the recording setting page. In this page, you can define the recording source, recording schedule and recording capacity. A total of 2 recording settings can be configured.



Recording

Recording name: Video

☑ Enable this recording

Priority: Normal

Source: Stream1

Recording Schedule

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time

● Always

○ From 00:00 to 24:00 [hh:mm]

Destination NAS

Capacity:

○ Entire free space

● Limit recording size in 1000 Mbytes

File name prefix: Video_

☑ Enable cyclic recording

Reserved amount: 15 Mbytes

Note: To enable recording notification please configure Application first

Recording name: Enter a descriptive name for the recording setting.

Enable this recording: Select this option to enable video recording.

Priority: Select the relative importance of this recording setting (High, Normal, and Low).

Source: Select the recording source (stream 1 or stream 2).

Recording Schedule: Specify the recording duration.

■ Select the days on weekly basis.

■ Select the time for recording in 24-hr time format.

Destination: Select a network storage you've setup for the recorded video files.

Capacity: You can choose either the entire free space or limit recording size. The limit recording size must larger than the reserved amount for cyclic recording.

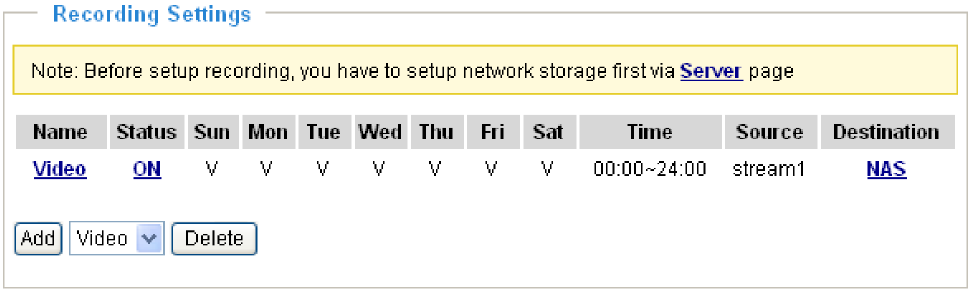
File name prefix: Enter the text that will be put in front of the file name.

Enable cyclic recording: If you check this item, when the maximum capacity is reached, the oldest file will be overwritten by the latest one. The reserved amount is reserverd for cyclic recording to prevent malfunction. This value must larger than 15 MBytes.

If you want to enable recording notification, please click **Application** to set up. Please refer to **Trigger > Recording notify** on page 68 for detailed information.

When completed, select **Enable this recording**. Click **Save** to take effect and then click **Close** to quit this page. The system begins recording and send recorded files to the Network Storage.
The new recording name will appear in the recording drop-down list on the recording page as below.

To remove a recording setting from the list, select a recording name from the drop-down list and then click **Delete**.



Recording Settings

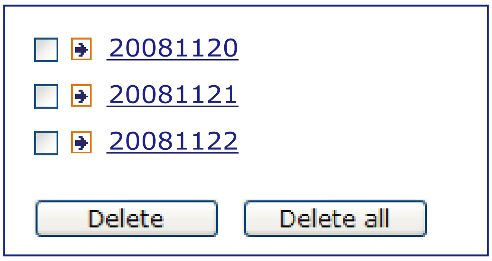
Note: Before setup recording, you have to setup network storage first via Server page

Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Source	Destination
Video	ON	V	V	V	V	V	V	V	00:00~24:00	stream1	NAS

■ Click **Video**: Open the Recording Settings page to modify.

■ Click **ON**: The Status will become **OFF** and stop recording.

■ Click **NAS**: Open the recorded file list as below. For more information about folder naming rule, please refer to page 77 for details.

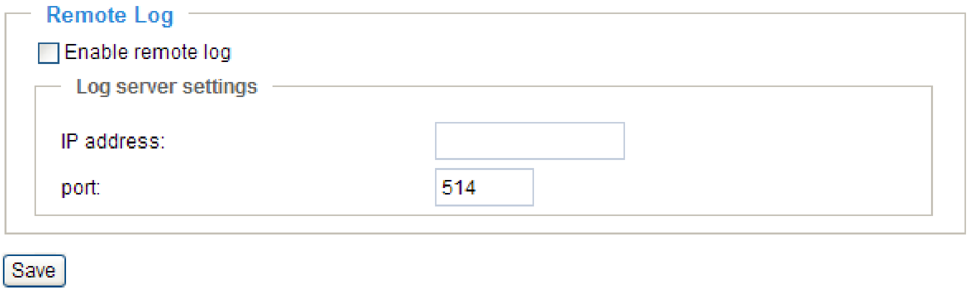


□ 20081120
□ 20081121
□ 20081122

System log Advanced mode

This section explains how to configure the Network Camera to send system log to the remote server as a backup.

Remote Log



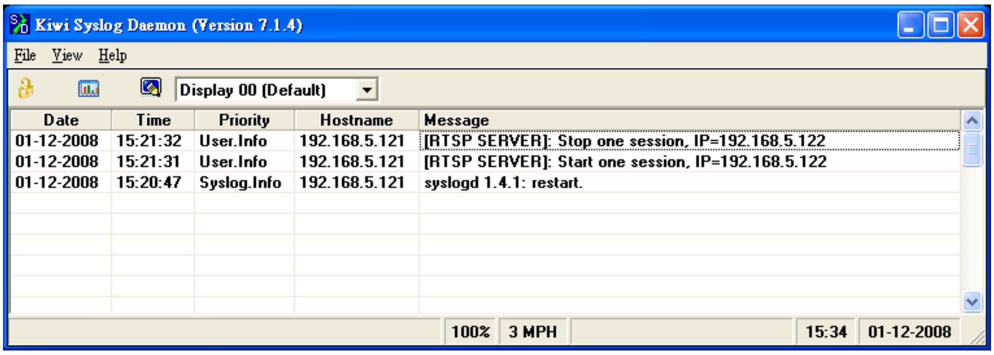
Remote Log

□ Enable remote log

Log server settings

IP address:	
port:	514

You can configure the Network Camera to send the system log file to a remote server as a log backup. Before utilizing this feature, it is suggested to install a log-recording tool to receive system log messages from the Network Camera. For example, a tool -- Kiwi Syslog Daemon. Visit http://www.kiwisyslog.com/kiwi-syslog-daemon-overview/.



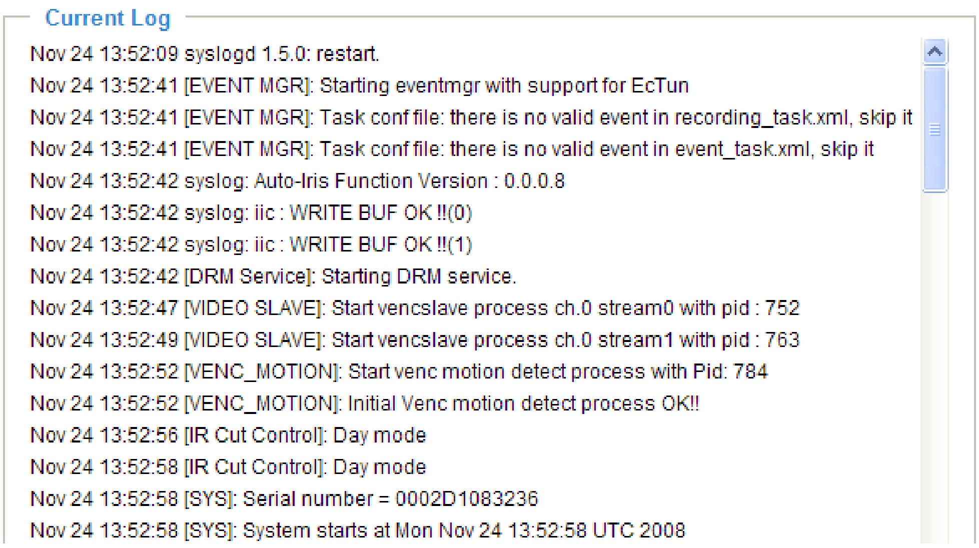
Kiwi Syslog Daemon (Version 7.1.4)
File View Help
Display 00 (Default)

Date	Time	Priority	Hostname	Message
01-12-2008	15:21:32	User.Info	192.168.5.121	[RTSP SERVER]: Stop one session, IP=192.168.5.122
01-12-2008	15:21:31	User.Info	192.168.5.121	[RTSP SERVER]: Start one session, IP=192.168.5.122
01-12-2008	15:20:47	Syslog.Info	192.168.5.121	syslogd 1.4.1: restart.

100% 3 MPH 15:34 01-12-2008

Follow the steps below to set up the remote log:
1. In the IP address text box, enter the IP address of the remote server.
2. In the port text box, enter the port number of the remote server.
3. When completed, select **Enable remote log** and click **Save** to take effect.

Current Log



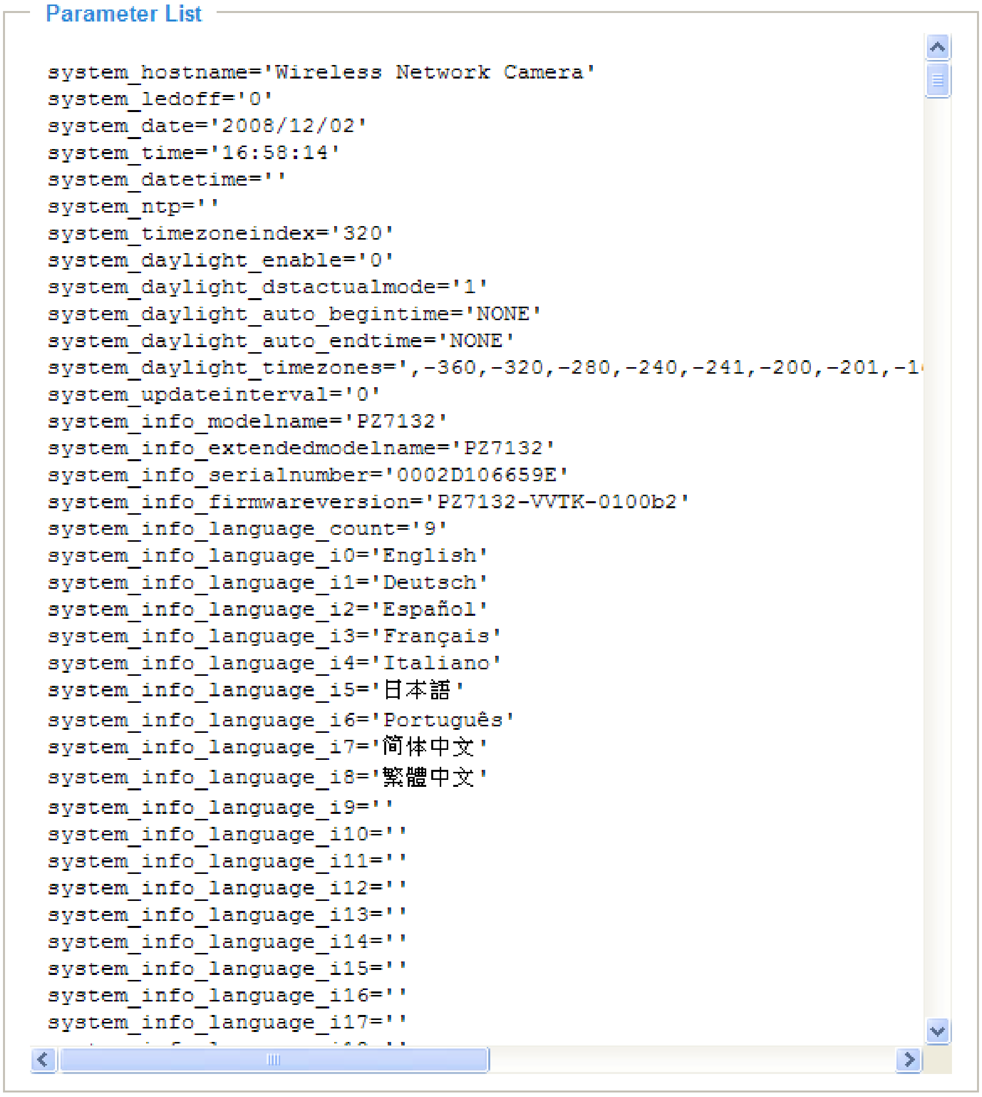
Current Log

```
Nov 24 13:52:09 syslogd 1.5.0: restart.
Nov 24 13:52:41 [EVENT MGR]: Starting eventmgr with support for EcTun
Nov 24 13:52:41 [EVENT MGR]: Task conf file: there is no valid event in recording_task.xml, skip it
Nov 24 13:52:41 [EVENT MGR]: Task conf file: there is no valid event in event_task.xml, skip it
Nov 24 13:52:42 syslog: Auto-Iris Function Version : 0.0.0.8
Nov 24 13:52:42 syslog: iic : WRITE BUF OK !!(0)
Nov 24 13:52:42 syslog: iic : WRITE BUF OK !!(1)
Nov 24 13:52:42 [DRM Service]: Starting DRM service.
Nov 24 13:52:47 [VIDEO SLAVE]: Start vencslave process ch.0 stream0 with pid : 752
Nov 24 13:52:49 [VIDEO SLAVE]: Start vencslave process ch.0 stream1 with pid : 763
Nov 24 13:52:52 [VENC_MOTION]: Start venc motion detect process with Pid: 784
Nov 24 13:52:52 [VENC_MOTION]: Initial Venc motion detect process OK!!
Nov 24 13:52:56 [IR Cut Control]: Day mode
Nov 24 13:52:58 [IR Cut Control]: Day mode
Nov 24 13:52:58 [SYS]: Serial number = 0002D1083236
Nov 24 13:52:58 [SYS]: System starts at Mon Nov 24 13:52:58 UTC 2008
```

This column displays the system's log in chronological order. The system log is stored in the Network Camera's buffer area and will be overwritten when reaching a certain amount.

View parameters Advanced mode

The View parameters page lists the entire system's parameters in alphabetical order. If you need technical assistance, please provide the information listed in this page.



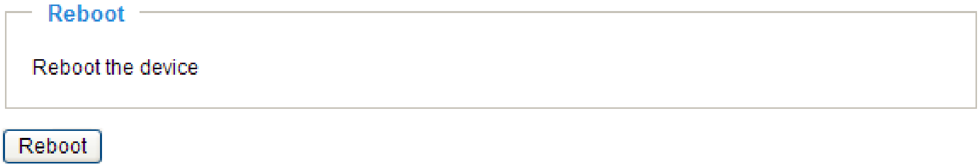
Parameter List

```
system_hostname='Wireless Network Camera'
system_ledoff='0'
system_date='2008/12/02'
system_time='16:58:14'
system_datetime=''
system_ntp=''
system_timezoneindex='320'
system_daylight_enable='0'
system_daylight_dstactualmode='1'
system_daylight_auto_begintime='NONE'
system_daylight_auto_endtime='NONE'
system_daylight_timezones=',-360,-320,-280,-240,-241,-200,-201,-1
system_updateinterval='0'
system_info_modelname='PZ7132'
system_info_extendedmodelname='PZ7132'
system_info_serialnumber='0002D106659E'
system_info_firmwareversion='PZ7132-VVTK-0100b2'
system_info_language_count='9'
system_info_language_i0='English'
system_info_language_i1='Deutsch'
system_info_language_i2='Español'
system_info_language_i3='Français'
system_info_language_i4='Italiano'
system_info_language_i5='日本語'
system_info_language_i6='Português'
system_info_language_i7='简体中文'
system_info_language_i8='繁體中文'
system_info_language_i9=''
system_info_language_i10=''
system_info_language_i11=''
system_info_language_i12=''
system_info_language_i13=''
system_info_language_i14=''
system_info_language_i15=''
system_info_language_i16=''
system_info_language_i17=''
```

Maintenance

This chapter explains how to restore the Network Camera to factory default, upgrade firmware version, etc.

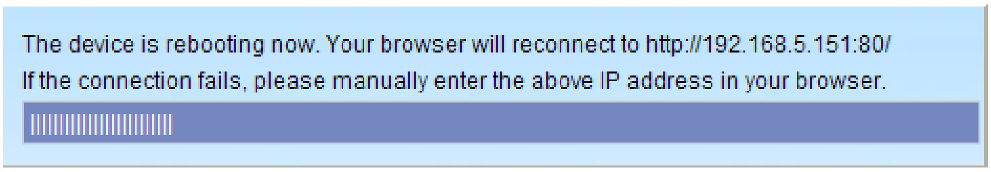
Reboot



Reboot

Reboot the device

This feature allows you to reboot the Network Camera, which takes about one minute to complete. When completed, the live video page will be displayed in your browser. The following message will show during the rebooting process.

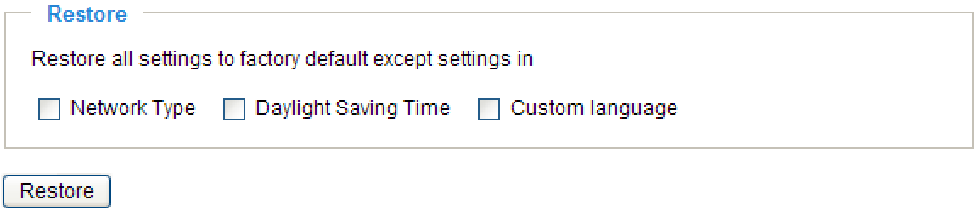


The device is rebooting now. Your browser will reconnect to http://192.168.5.151:80/

If the connection fails, please manually enter the above IP address in your browser.

If the connection fails after rebooting, manually enter the IP address of the Network Camera in the address field to resume the connection.

Restore



Restore

Restore all settings to factory default except settings in

□ Network Type □ Daylight Saving Time □ Custom language

This feature allows you to restore the Network Camera to factory default.

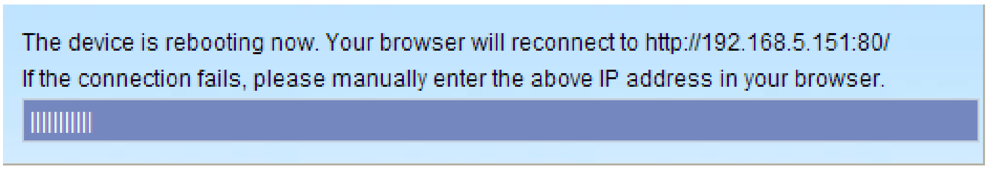
Network Type: Select this option to retain the Network Type settings. (Please refer to Network Type on page 33.)

Daylight Saving Time: Select this option to retain the Daylight Saving Time settings. (Please refer to System on page 25.)

Custom language: Select this option to retain the Custom language settings.

If none of the options is selected, all settings will be restored to factory default.

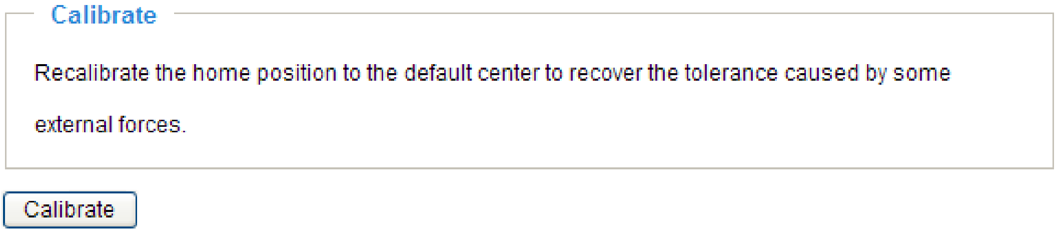
The following message is displayed during the restoring process.



The device is rebooting now. Your browser will reconnect to http://192.168.5.151:80/

If the connection fails, please manually enter the above IP address in your browser.

Calibrate



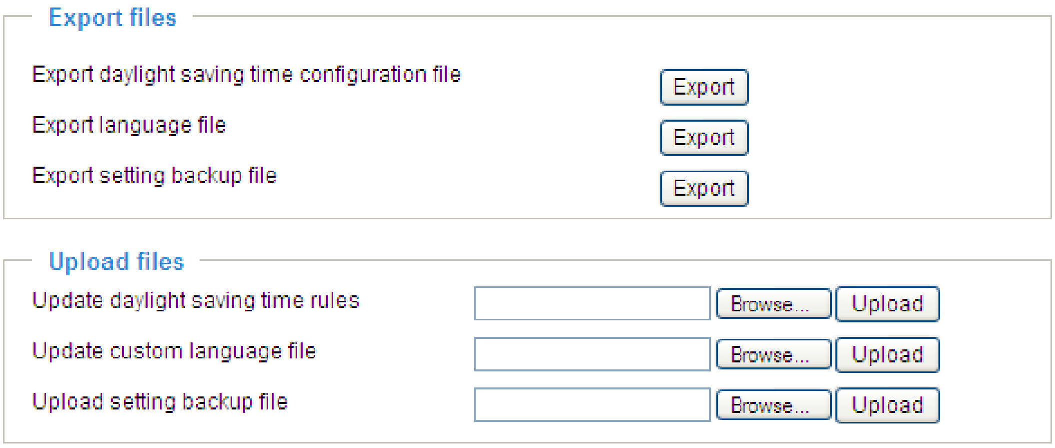
Calibrate

Recalibrate the home position to the default center to recover the tolerance caused by some external forces.

This feature re-calibrate the home position to the default center to recover the tolerance caused by some external forces. Please note that there is no confirming message box after clicking on **Calibrate**, the Network Camera will calibrate immediately.

Export / Upload Files Advanced mode

This feature allows you to Export / Upload daylight saving time rules, custom language files, and setting backup files.



Export files

Export daylight saving time configuration file

Export language file

Export setting backup file

Upload files

Update daylight saving time rules

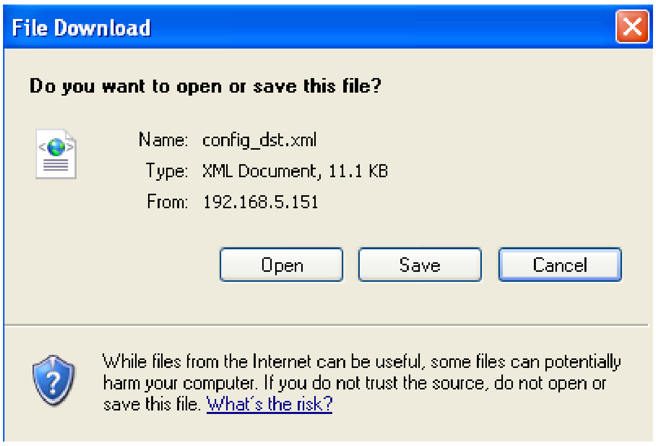
Update custom language file

Upload setting backup file

Export daylight saving time configuration file: Click to set the starting time and ending time of DST.

Follow the steps below to export:

1. In the Export files column, click **Export** to export a daylight saving time configuration file from the Network Camera.
2. A File Download dialog will pop up as below. Click **Open** to review the XML file or click **Save** to store the file for further settings.



File Download

Do you want to open or save this file?

Name: config_dst.xml

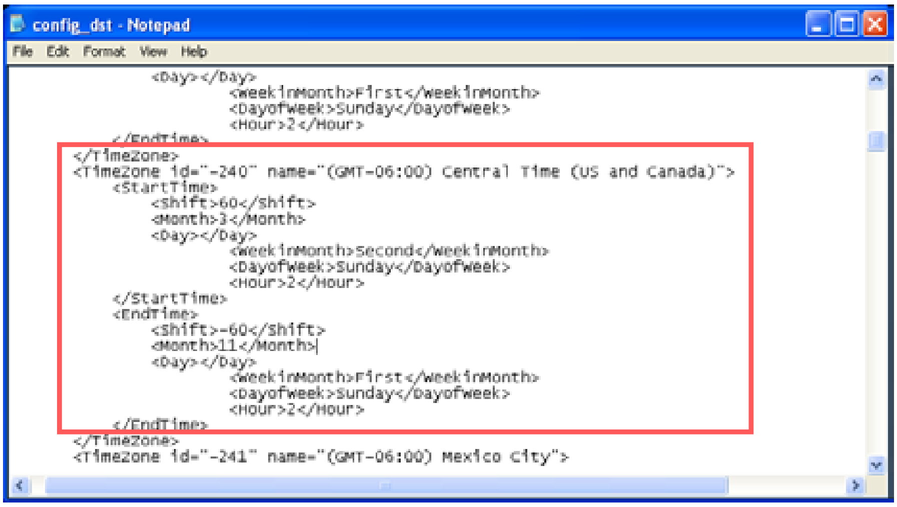
Type: XML Document, 11.1 KB

From: 192.168.5.151

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

3. Open the file with Microsoft® Notepad and locate your time zone; set the starting time and ending time of the DST. When completed, save the file.

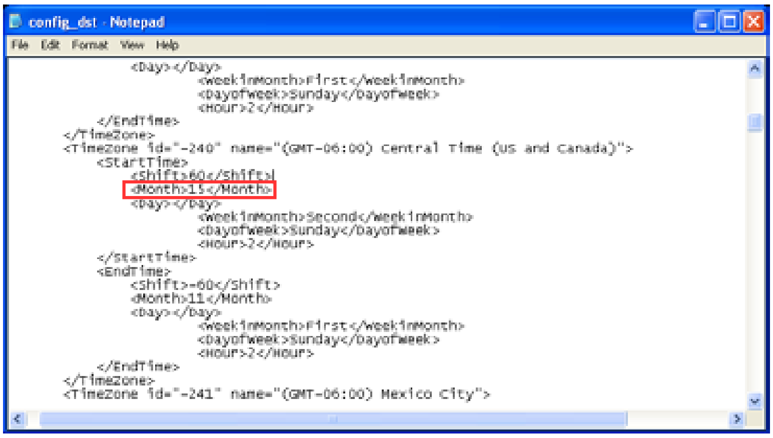
In the example below, the DST begins each year at 2:00 a.m. on the second Sunday in March and ends at 2:00 a.m. on the first Sunday in November.



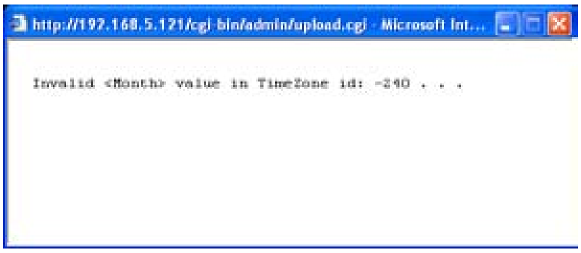
```
            <Day></Day>
                    <WeekInMonth>First</WeekInMonth>
                    <DayofWeek>Sunday</DayofWeek>
                    <Hour>2</Hour>
        </EndTime>
    </TimeZone>
    <TimeZone id="-240" name="(GMT-06:00) Central Time (US and Canada)">
        <StartTime>
            <Shift>60</Shift>
            <Month>3</Month>
            <Day></Day>
                    <WeekInMonth>Second</WeekInMonth>
                    <DayofWeek>Sunday</DayofWeek>
                    <Hour>2</Hour>
        </StartTime>
        <EndTime>
            <Shift>-60</Shift>
            <Month>11</Month>
            <Day></Day>
                    <WeekInMonth>First</WeekInMonth>
                    <DayofWeek>Sunday</DayofWeek>
                    <Hour>2</Hour>
        </EndTime>
    </TimeZone>
    <TimeZone id="-241" name="(GMT-06:00) Mexico City">
```

Upload daylight saving time rule: Click **Browse…** and specify the XML file to upload.

If the incorrect date and time is assigned, you will see the following warning message when uploading the file to the Network Camera.

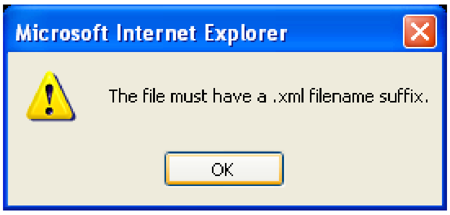


```
            <Day></Day>
                    <WeekInMonth>First</WeekInMonth>
                    <DayofWeek>Sunday</DayofWeek>
                    <Hour>2</Hour>
        </EndTime>
    </TimeZone>
    <TimeZone id="-240" name="(GMT-06:00) Central Time (US and Canada)">
        <StartTime>
            <Shift>60</Shift>
            <Month>15</Month>
            <Day></Day>
                    <WeekInMonth>Second</WeekInMonth>
                    <DayofWeek>Sunday</DayofWeek>
                    <Hour>2</Hour>
        </StartTime>
        <EndTime>
            <Shift>-60</Shift>
            <Month>11</Month>
            <Day></Day>
                    <WeekInMonth>First</WeekInMonth>
                    <DayofWeek>Sunday</DayofWeek>
                    <Hour>2</Hour>
        </EndTime>
    </TimeZone>
    <TimeZone id="-241" name="(GMT-06:00) Mexico City">
```


http://192.168.5.121/cgi-bin/admin/upload.cgi - Microsoft Int...

```
Invalid <Month> value in TimeZone id: -240 . . .
```

The following message is displayed when attempting to upload an incorrect file format.



The file must have a .xml filename suffix.

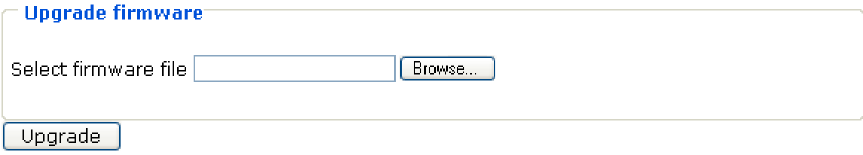
Export language file: Click to export language strings. VIVOTEK provides nine languages: English, Deutsch, Español, Français, Italiano, 日本語, Português, 簡体中文, and 繁體中文.

Upload custom language file: Click **Browse…** and specify your own custom language file to upload.

Export setting backup file: Click to export all parameters of the device and user-defined script.

Upload setting backup file: Click **Browse…** to upload a setting backup file. Please note that the model and firmware version of the device should be the same as the setting backup file. If you have set up fixed IP or other special settings for your device, it is not suggested to upload a settings backup file.

Upgrade Firmware

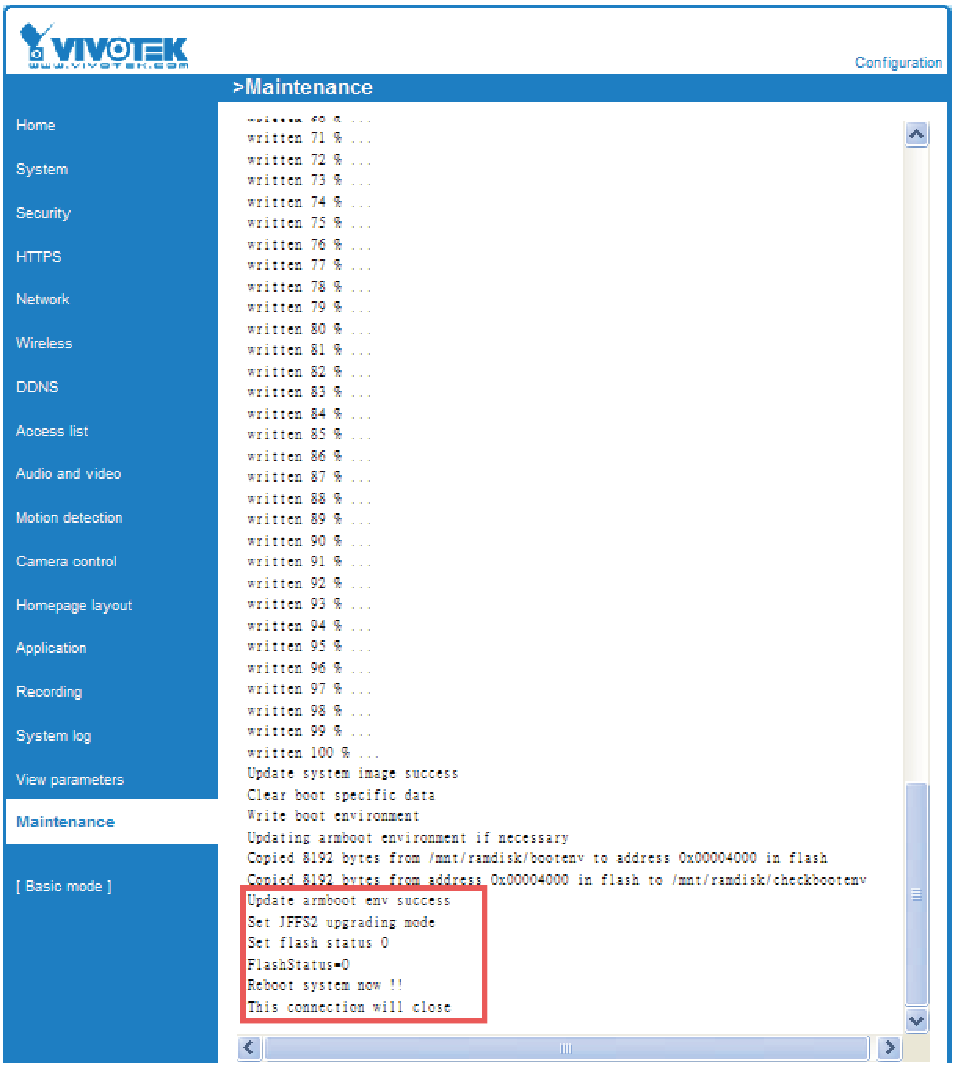


This feature allows you to upgrade the firmware on your Network Camera. It takes a few minutes to complete the process.
Note that do not power off the Network Camera during the upgrade.

Follow the steps below to upgrade firmware:
1. Download a new firmware file from VIVOTEK website. The file is in .pkg file format.
2. Click **Browse…** and specify the firmware file.
3. Click **Upgrade**. The Network Camera starts to upgrade and will reboot automatically when the upgrade completes.

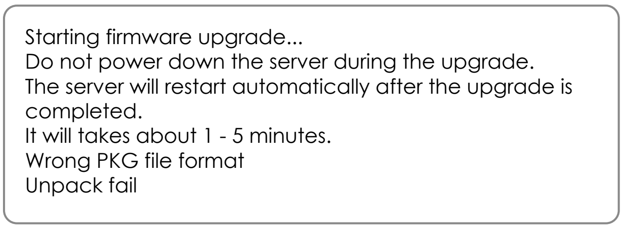
The upgrade is successful as you see “Reboot system now!! This connection will close”. After that, re-access the Network Camera.

The following message is displayed when the upgrade is succeeded.



```
written 70 % ...
written 71 % ...
written 72 % ...
written 73 % ...
written 74 % ...
written 75 % ...
written 76 % ...
written 77 % ...
written 78 % ...
written 79 % ...
written 80 % ...
written 81 % ...
written 82 % ...
written 83 % ...
written 84 % ...
written 85 % ...
written 86 % ...
written 87 % ...
written 88 % ...
written 89 % ...
written 90 % ...
written 91 % ...
written 92 % ...
written 93 % ...
written 94 % ...
written 95 % ...
written 96 % ...
written 97 % ...
written 98 % ...
written 99 % ...
written 100 % ...
Update system image success
Clear boot specific data
Write boot environment
Updating armboot environment if necessary
Copied 8192 bytes from /mnt/ramdisk/bootenv to address 0x00004000 in flash
Copied 8192 bytes from address 0x00004000 in flash to /mnt/ramdisk/checkbootenv
Update armboot env success
Set JFFS2 upgrading mode
Set flash status 0
FlashStatus=0
Reboot system now !!
This connection will close
```

The following message is displayed when you have selected an incorrect firmware file.



Starting firmware upgrade...
Do not power down the server during the upgrade.
The server will restart automatically after the upgrade is completed.
It will takes about 1 - 5 minutes.
Wrong PKG file format
Unpack fail

Appendix

URL Commands of the Network Camera

Overview

For some customers who already have their own web site or web control application, Network Camera/ Video server can be easily integrated through convenient URLs. This section specifies the external HTTP based application programming interface. The HTTP based camera interface provides the functionality to request a single image, to control camera functions (PTZ, output relay etc.) and to get and set internal parameter values. The image and CGI-requests are handled by the built in Web server.

Style convention

In URL syntax and in descriptions of CGI parameters, a text within angle brackets denotes a content that is to be replaced with either a value or a string. When replacing the text string also the angle brackets shall be replaced. An example of this is the description of the name for the server, denoted with <servername> in the URL syntax description below, that is replaced with the string myserver in the URL syntax example, also below.

URL syntax' are written with the “**Syntax:**" word written in bold face followed by a box with the referred syntax as seen below. The name of the server is written as <servername>. This is intended to be replaced with the name of the actual server. This can either be a name, e.g., "mywebcam" or "thecam.adomain.net" or the associated IP number for the server, e.g., 192.168.0.220.

Syntax:

```
http://<servername>/cgi-bin/viewer/video.jpg
```

Description of returned data is written with "**Return:**" in bold face followed by the returned data in a box. All data returned as HTTP formatted, i.e., starting with the string HTTP is line separated with a Carriage Return and Line Feed (CRLF) printed as \r\n.

Return:

```
HTTP/1.0 <HTTP code> <HTTP text>\r\n
```

URL syntax examples are written with "**Example:**" in bold face followed by a short description and a light grey box with the example.

Example: request a single snapshot image

```
http://mywebserver/cgi-bin/viewer/video.jpg
```

General CGI URL syntax and parameters

CGI parameters are written in lower-case and as one word without any underscores or other separators. When the CGI request includes internal camera parameters, the internal parameters must be written exactly as they are named in the camera or video server. The CGIs are organized in function related directories under the cgi-bin directory. The file extension of the CGI is required.

Syntax:

```
http://<servername>/cgi-bin/<subdir>[/<subdir>...]/<cgi>.<ext>
[?<parameter>=<value>[&<parameter>=<value>...]]
```

Example: Setting digital output #1 to active

```
http://mywebserver/cgi-bin/dido/setdo.cgi?do1=1
```

Security level

SECURITY LEVEL	SUB-DIRECTORY	DESCRIPTION
0	anonymous	Unprotected.
1 [view]	anonymous, viewer, dido, camctrl	1. Can view, listen, talk to camera 2. Can control dido, ptz of camera
4 [operator]	anonymous, viewer, dido, camctrl, operator	Operator's access right can modify most of camera's parameters except some privilege and network options
6 [admin]	anonymous, viewer, dido, camctrl, operator, admin	Administrator's access right can fully control the camera's operation.
7	N/A	Internal parameters. Unable to be changed by any external interface.

Get server parameter values

Note: The access right depends on the URL directory.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/anonymous/getparam.cgi?[<parameter>]
[&<parameter>…]
```

```
http://<servername>/cgi-bin/viewer/getparam.cgi?[<parameter>]
[&<parameter>…]

http://<servername>/cgi-bin/operator/getparam.cgi?[<parameter>]
[&<parameter>…]

http://<servername>/cgi-bin/admin/getparam.cgi?[<parameter>]
[&<parameter>…]
```

where the *<parameter>* should be *<group>*[_*<name>*] or *<group>*[.*<name>*] If you do not specify the any parameters, all the parameters on the server will be returned. If you specify only *<group>*, the parameters of related group will be returned.

When query parameter values, the current parameter value are returned.
Successful control request returns paramter pairs as follows.
Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: <length>\r\n
\r\n
<parameter pair>
```

where <parameter pair> is
<parameter>=<value>\r\n
[<parameter pair>]

<length> is the actual length of content.

Example: request IP address and it's response

```
Request:
http://192.168.0.123/cgi-bin/admin/getparam.cgi?network_ipaddress

Response:
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: 33\r\n
\r\n
network.ipaddress=192.168.0.123\r\n
```

Set server parameter values

Note: The access right depends on the URL directory.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/anonymous/setparam.cgi? <parameter>=<value>
[&<parameter>=<value>…][&update=<value>][&return=<return page>]

http://<servername>/cgi-bin/viewer/setparam.cgi? <parameter>=<value>
[&<parameter>=<value>…][&update=<value>] [&return=<return page>]

http://<servername>/cgi-bin/operator/setparam.cgi? <parameter>=<value>
[&<parameter>=<value>…][&update=<value>] [&return=<return page>]

http://<servername>/cgi-bin/admin/setparam.cgi? <parameter>=<value>
[&<parameter>=<value>…][&update=<value>] [&return=<return page>]
```

PARAMETER	VALUE	DESCRIPTION
<group>_<name>	value to assigned	Assign *<value>* to the parameter *<group>_<name>*
update	<boolean>	set to 1 to actually update all fields (no need to use update parameter in each group)
return	*<return page>*	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according the the current path. If you omit this parameter, it will redirect to an empty page. (note: The return page can be a general HTML file(.htm, .html) or a Vivotek server script executable (.vspx) file. It can not be a CGI command. It can not have any extra parameters. This parameter must be put at end of parameter list)

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: <length>\r\n
```

```
\r\n
<parameter pair>
```

where <parameter pair> is

<parameter>=<value>\r\n

[<parameter pair>]

Only the parameters that you set and readable will be returned.

Example: Set the IP address of server to 192.168.0.123

```
Request:
http://myserver/cgi-bin/admin/setparam.cgi?network_ipaddress=192.168.0.123

Response:
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: 33\r\n
\r\n
network.ipaddress=192.168.0.123\r\n
```

Available parameters on the server

Valid values:

VALID VALUES	DESCRIPTION
string[<n>]	Text string shorter than ‘n’ characters. The characters “,’, <,>,& are invalid.
password[<n>]	The same as string but display ‘*’ instead
integer	Any number between $(-2^{31} - 1)$ and $(2^{31} - 1)$
positive integer	Any number between 0 and $(2^{32} - 1)$
<m> ~ <n>	Any number between ‘m’ and ‘n’
domain name[<n>]	A string limited to contain a domain name shorter than ‘n’ characters (eg. www.ibm.com)
email address [<n>]	A string limited to contain a email address shorter than ‘n’ characters (eg. joe@www.ibm.com)
ip address	A string limited to contain an ip address (eg. 192.168.1.1)
mac address	A string limited to contain mac address without hyphen or colon connected
boolean	A boolean value 1 or 0 represents [Yes or No], [True or False], [Enable or Disable].
<value1>, <value2>,	Enumeration. Only given values are valid.

<value3>, …	
blank	A blank string
everything inside <>	As description

NOTE: The camera should prevent to restart when parameter changed.

Group: **system**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
hostname	string[40]	1/6	host name of server (Network Camera, Wireless Network Camera)
ledoff	<boolean>	6/6	turn on(0) or turn off(1) all led indicators
date	<yyyy/mm/dd>, keep, auto	6/6	Current date of system. Set to ‘keep’ keeping date unchanged. Set to ‘auto’ to use NTP to synchronize date.
time	<hh:mm:ss>, keep, auto	6/6	Current time of system. Set to ‘keep’ keeping time unchanged. Set to ‘auto’ to use NTP to synchronize time.
datetime	<MMDDhhmmYYYY.ss>	6/6	Another current time format of system.
ntp	<domain name>, <ip address>, <blank>	6/6	NTP server *do not use “skip to invoke default server” for default
timezoneindex	-489 ~ 529	6/6	Indicate timezone and area -480: GMT-12:00 Eniwetok, Kwajalein -440: GMT-11:00 Midway Island, Samoa -400: GMT-10:00 Hawaii -360: GMT-09:00 Alaska -320: GMT-08:00 Las Vegas, San_Francisco, Vancouver -280: GMT-07:00 Mountain Time, Denver -281: GMT-07:00 Arizona -240: GMT-06:00 Central America, Central Time, Mexico City, Saskatchewan -200: GMT-05:00 Eastern Time, New York, Toronto -201: GMT-05:00 Bogota, Lima, Quito,

			Indiana -160: GMT-04:00 Atlantic Time, Canada, Caracas, La Paz, Santiago -140: GMT-03:30 Newfoundland -120: GMT-03:00 Brasilia, Buenos Aires, Georgetown, Greenland -80: GMT-02:00 Mid-Atlantic -40: GMT-01:00 Azores, Cape_Verde_IS. 0: GMT Casablanca, Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London 40: GMT 01:00 Amsterdam, Berlin, Rome, Stockholm, Vienna, Madrid, Paris 41: GMT 01:00 Warsaw, Budapest, Bern 80: GMT 02:00 Athens, Helsinki, Istanbul, Riga 81: GMT 02:00 Cairo 82: GMT 02:00 Lebanon, Minsk 83: GMT 02:00 Israel 120: GMT 03:00 Baghdad, Kuwait, Riyadh, Moscow, St. Petersburg, Nairobi 121: GMT 03:00 Iraq 140: GMT 03:30 Tehran 160: GMT 04:00 Abu Dhabi, Muscat, Baku, Tbilisi, Yerevan 180: GMT 04:30 Kabul 200: GMT 05:00 Ekaterinburg, Islamabad, Karachi, Tashkent 220: GMT 05:30 Calcutta, Chennai, Mumbai, New Delhi 230: GMT 05:45 Kathmandu 240: GMT 06:00 Almaty, Novosibirsk, Astana, Dhaka, Sri Jayawardenepura 260: GMT 06:30 Rangoon 280: GMT 07:00 Bangkok, Hanoi, Jakarta, Krasnoyarsk 320: GMT 08:00 Beijing, Chongging, Hong Kong, Kuala Lumpur, Singapore, Taipei 360: GMT 09:00 Osaka, Sapporo, Tokyo,

			Seoul, Yakutsk 380: GMT 09:30 Adelaide, Darwin 400: GMT 10:00 Brisbane, Canberra, Melbourne, Sydney, Guam, Vladivostok 440: GMT 11:00 Magadan, Solomon Is., New Caledonia 480: GMT 12:00 Aucklan, Wellington, Fiji, Kamchatka, Marshall Is. 520: GMT 13:00 Nuku'Alofa
daylight_enable	<boolean>	6/6	enable automatic daylight saving to time zone
daylight_dstactualmode	<boolean>	6/7	check if current time is under daylight saving time.
daylight_auto_begintime	string[19]	6/7	display the current daylight saving begin time. (product dependent)
daylight_auto_endtime	string[19]	6/7	display the current daylight saving end time. (product dependent)
updateinterval	0, 3600, 86400, 604800, 2592000	6/6	0 to Disable automatic time adjustment, otherwise, it means the seconds between NTP automatic update interval.
restore	0, <positive integer>	7/6	Restore the system parameters to default value after <value> seconds.
reset	0, <positive integer>	7/6	Restart the server after <value> seconds if <value> is non-negative.
restoreexceptnet	<Any value>	7/6	Restore the system parameters to default value except (ipaddress, subnet, router, dns1, dns2, pppoe). This command can cooperate with other “restoreexceptXYZ” commands. When cooperating with others, the system parameters will be restored to default value except a union of combined results.
restoreexceptdst	<Any value>	7/6	Restore the system parameters to default value except all daylight saving time

			settings. This command can cooperate with other "restoreexceptXYZ" commands. When cooperating with others, the system parameters will be restored to default value except a union of combined results.
restoreexceptlang	<Any Value>	7/6	Restore the system parameters to default value except custom language file user uploaded. This command can cooperate with other "restoreexceptXYZ" commands. When cooperating with others, the system parameters will be restored to default value except a union of combined results.

SubGroup of **system**: **info** (The fields in this group are unchangeable.)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
modelname	string[40]	0/7	Internal model name of server (eg. IP7139)
extendedmodelname	string[40]	0/7	ODM specific model name of server (eg. DCS-5610). If it is not ODM case, this field will be equal to "modelname"
serialnumber	<mac address>	0/7	12 characters mac address without hyphen connected
firmwareversion	string[40]	0/7	The version of firmware, including model, company, and version number in the format <MODEL-BRAND-VERSION>
language_count	<integer>	0/7	number of webpage language available on the server
language_i<0~(count-1)>	string[16]	0/7	Available language lists
customlanguage_maxcount	<integer>	0/7	Maximum number of custom language supported on the server
customlanguage_count	<integer>	0/7	Number of custom language which has been uploaded to the server
customlanguage_i<0~(max count-1)>	string	0/7	Custom language name

Group: **status**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
di_i<0~(ndi-1)>	<boolean>	1/7	0 => Inactive, normal 1 => Active, triggered
do_i<0~ndi-1)>	<boolean>	1/7	0 => Inactive, normal 1 => Active, triggered
onlinenum_rtsp	integer	6/7	current RTSP connection numbers
onlinenum_httppush	integer	6/7	current HTTP push server connection numbers

Group: **di_i<0~(ndi-1)>** (capability.ndi > 0)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
normalstate	high, low	1/1	indicate whether open circuit or closed circuit represents inactive status

Group: **do_i<0~(ndo-1)>** (capability.ndo > 0)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
normalstate	open, grounded	1/1	indicate whether open circuit or closed circuit represents inactive status

Group: security

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
privilege_do	view, operator, admin	6/6	Indicate which privilege and above can control digital output
privilege_camctrl	view, operator, admin	6/6	Indicate which privilege and above can control PTZ
user_i0_name	string[64]	6/7	User's name of root
user_i<1~20>_name	string[64]	6/7	User's name
user_i0_pass	password[64]	6/6	root's password
user_i<1~20>_pass	password[64]	7/6	User's password
user_i0_privilege	viewer, operator, admin	6/7	root's privilege
user_i<1~20>_privilege	viewer, operator, admin	6/6	User's privilege.

Group: **network**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
type	lan, pppoe	6/6	Network connection type
resetip	<boolean>	6/6	1 => get ipaddress, subnet, router, dns1, dns2 from DHCP server at next reboot 0 => use preset ipaddress, subnet, rounter, dns1, and dns2
ipaddress	<ip address>	6/6	IP address of server
subnet	<ip address>	6/6	subnet mask
router	<ip address>	6/6	default gateway
dns1	<ip address>	6/6	primary DNS server
dns2	<ip address>	6/6	secondary DNS server
wins1	<ip address>	6/6	primary WINS server
wins2	<ip address>	6/6	secondary WINS server

Subgroup of **network**: **ipv6**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	6/6	Enable IPv6
addonipaddress	<ip address>	6/6	IPv6 IP address
addonprefixlen	0~128	6/6	IPv6 prefix length
addonrouter	<ip address>	6/6	IPv6 router address
addondns	<ip address>	6/6	IPv6 DNS address
allowoptional	<boolean>	6/6	Allow Manually setup the IP address setting

Subgroup of **network**: **ftp**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
port	21, 1025~65535	6/6	local ftp server port

Subgroup of **network**: **http**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
port	80, 1025 ~ 65535	6/6	HTTP port
alternateport	1025~65535	6/6	Alternative HTTP port
authmode	basic,	1/6	HTTP authentication mode

	digest		
s0_accessname	string[32]	1/6	Http server push access name for stream 1 (capability.protocol.spush_mjpeg =1 and video.stream.count>0)
s1_accessname	string[32]	1/6	Http server push access name for stream 2 (capability.protocol.spush_mjpeg =1 and video.stream.count>1)
anonymousviewing	<boolean>	1/6	Enable anoymous streaming viewing.

Subgroup of **network**: **https**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
port	443, 1025 ~ 65535	6/6	HTTPS port

Subgroup of **network**: **rtsp**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
port	554, 1025 ~ 65535	1/6	RTSP port (capability.protocol.rtsp=1)
anonymousviewing	<boolean>	1/6	Enable anoymous streaming viewing.
authmode	disable, basic, digest	1/6	RTSP authentication mode (capability.protocol.rtsp=1)
s0_accessname	string[3b;42]	1/6	RTSP access name for stream1 (capability.protocol.rtsp=1 and video.stream.count>0)
s1_accessname	string[32]	1/6	RTSP access name for stream2 (capability.protocol.rtsp=1 and video.stream.count>1)
s0_audiotrack	<integer>	6/6	The current audio track for stream1. -1 => audio mute
s1_audiotrack	<integer>	6/6	The current audio track for stream2. -1 => audio mute

Subgroup of **rtsp_s<0~(n-1)>**: **multicast,** n is stream count (capability.protocol.rtp.multicast=1)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
alwaysmulticast	<boolean>	4/4	Enable always multicast
ipaddress	<ip address>	4/4	Multicast IP address
videoport	1025 ~ 65535	4/4	Multicast video port
audioport	1025 ~ 65535	4/4	Multicast audio port
ttl	1 ~ 255	4/4	Mutlicast time to live value

Subgroup of **network**: **sip**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
port	1025 ~ 65535	6/6	SIP port (capability.protocol.sip=1)

Subgroup of **network**: **rtp**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
videoport	1025 ~ 65535	6/6	video channel port for RTP (capability.protocol.rtp_unicast=1)
audioport	1025 ~ 65535	6/6	audio channel port for RTP (capability.protocol.rtp_unicast=1)

Subgroup of **network**: **pppoe**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
user	string[128]	6/6	PPPoE account user name
pass	password[64]	6/6	PPPoE account password

Group: **wireless**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
ssid	string[32]	6/6	SSID for wireless lan settings. The valid characters are [A-Z] [a-z] [0-9] [/] [.] [_] [=] [ ] [-] [+] [*].
wlmode	Infra,	6/6	wireless mode

	Adhoc		Infra: Infrastructure
channel	1~11 or 1 ~ 13 or 10~11 or 10~13 or 1~14	6/6	USA and Canada Europe Spain France All
txrate	NONE, 1M, 2M, 5.5M, 11M, 6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M, Auto	6/6	Maximum oolean rate in Mbps
encrypt	0~3	6/6	encryption method (product depedent) 0=> NONE, 1 => WEP, 2 => WPA, 3 => WPA2PSK
authmode	OPEN, SHARED	6/6	Authentication mode
keylength	64, 128	6/6	key length in bits
keyformat	HEX, ASCII	6/6	key1 ~ key4 presentation format
keyselect	1 ~ 4	6/6	default key number
key1	password [32]	6/6	WEP key1 for encryption. The valid characters are [A-Z] [a-z] [0-9].
key2	password [32]	6/6	WEP key2 for encryption. The valid characters are [A-Z] [a-z] [0-9].
key3	password [32]	6/6	WEP key3 for encryption. The valid characters are [A-Z] [a-z] [0-9].
key4	password [32]	6/6	WEP key4 for encryption. The valid characters are [A-Z] [a-z] [0-9].
domain	‘U’ for USA ‘C’ for Canada ‘E’ for Euro ‘S’ for Spain ‘F’ for France ‘I’ for Isrel ‘A’ for All	6/7	Wireless domain
algorithm	AES, TKIP	6/6	Algorithm
presharedkey	password [63]	6/6	WPA mode pre-shared key. The valid characters are [A-Z] [a-z] [0-9].

Group: **ipfilter**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	6/6	Enable or disable ipfilter settings
admin_enable	<boolean>	6/6	Enable or disable the function always allow the admin IP address to access this device
admin_ip	1.0.0.0 ~ 255.255.255.255	6/6	Always allow this IP connect to camera when admin_enable=1
maxconnection	0~10	6/6	Maximum number of concurrent streaming connection(s) limit
allow_i<0~9>_start	1.0.0.0 ~ 255.255.255.255	6/6	Allowed starting IP address for RTSP connection
allow_i<0~9>_end	1.0.0.0 ~ 255.255.255.255	6/6	Allowed ending IP address for RTSP connection
deny_i<0~9>_start	1.0.0.0 ~ 255.255.255.255	6/6	Denied starting IP address for RTSP connection
deny_i<0~9>_end	1.0.0.0 ~ 255.255.255.255	6/6	Denied ending IP address for RTSP connection
ipv6_allow_i<0~9>_start	1.0.0.0 ~ 255.255.255.255	6/6	Allowed starting ipv6 IP address for RTSP connection
ipv6_allow_i<0~9>_end	1.0.0.0 ~ 255.255.255.255	6/6	Allowed ending ipv6 IP address for RTSP connection
ipv6_deny_i<0~9>_start	1.0.0.0 ~ 255.255.255.255	6/6	Denied starting ipv6 IP address for RTSP connection
ipv6_deny_i<0~9>_end	1.0.0.0 ~ 255.255.255.255	6/6	Denied ending ipv6 IP address for RTSP connection

Group: **videoin**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
cmosfreq	50, 60	4/4	CMOS frequency
whitebalance	auto, manual	4/4	auto, manual
atwbvalue	0 ~ 65535	4/4	The auto white balance value.
autoiris	0, 1	4/4	Enable auto Iris
enableblc	0, 1	4/4	Enable backlight compensation
agc	normal, max	4/4	Set auto gain control to normal level or MAX level
exposurelevel	1 ~ 8	4/4	Exposure level

Group: **videoin_c<0~(n-1)>** for n channel products, m is stream number

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
color	0, 1	4/4	0 =>monochrome 1 => color
flip	<boolean>	4/4	flip the image
mirror	<boolean>	4/4	mirror the image
text	string[16]	1/4	enclosed caption
imprinttimestamp	<boolean>	4/4	Overlay time stamp on video
maxexposure	1~120	4/4	Maximum exposure time
options	quality, framerate	4/4	To customize video quality first or video frame rate first. (product dependent)
s<0~(m-1)>_codectype	mpeg4, mjpeg	4/4	video codec type
s<0~(m-1)>_resolution	176x144, 320x240, 640x480	4/4	Video resolution in pixel
s<0~(m-1)>_mpeg4_intraperiod	250, 500, 1000, 2000, 3000, 4000	4/4	The period of intra frame in milliseconds
s<0~(m-1)>_mpeg4_ratecontrolmode	cbr, vbr	4/4	cbr, constant bitrate vbr, fix quality
s<0~(m-1)>_mpeg4_quant	0, 1~5	4/4	quality of video when choosing vbr in "ratecontrolmode". 0 is customized manual input setting. 1 is worst quality and 5 is the best quality.
s<0~(m-1)>_mpeg4_qvalue	1~31	7/4	The specific quality parameter of mpeg4 encoder. 1 is best quality and 31 is the worst quality.
s<0~(m-1)>_mpeg4_bitrate	1000~4000000	4/4	Set bit rate in bps when choose cbr in "ratecontrolmode"
s<0~(m-1)>_mpeg4_maxframe	1~30	4/4	set maximum frame rate in fps (for MPEG-4)

s<0~(m-1)>_mjpeg_quant	0 ~ 5	4/4	quality of jpeg video. 0 is customized manual input setting. 1 is worst quality and 5 is the best quality.
s<0~(m-1)>_mjpeg_ qvalue	10~200	7/4	The specific quality parameter of jpeg encoder. 10 is best quality and 200 is the worst quality.
s<0~(m-1)>_mjpeg_maxframe	1~30	4/4	set maximum frame rate in fps (for JPEG)
s<0~(m-1)>_forcei	1	7/6	Force I frame

Group: **audioin_c<0~(n-1)>** for n channel products (capability.audioin>0)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
source	micin, linein	4/4	micin => use external microphone input linein => use line input
mute	0, 1	4/4	Enable audio mute
gain	0~31	4/4	Gain of input
boostmic	0, 1	4/4	Enable microphone boost
s<0~(m-1)>_codectype	aac4, gamr	4/4	set audio codec type for input
s<0~(m-1)>_aac4_bitrate	16000, 32000, 48000, 64000, 96000, 128000	4/4	set AAC4 bitrate in bps
s<0~(m-1)>_gamr_bitrate	4750, 5150, 5900, 6700, 7400, 7950, 10200, 12200	4/4	set AMR bitrate in bps

Group: **image_c<0~(n-1)>** for n channel products

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
brightness	-5 ~ 5	4/4	Adjust brightness of image according to mode settings.
saturation	-5 ~ 5	4/4	Adjust saturation of image according to mode settings.
contrast	-5 ~ 5	4/4	Adjust contrast of image according to mode settings.
sharpness	-3 ~ 3	4/4	Adjust sharpness of image according to mode settings.

Group: **imagepreview**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
c<0~(n-1)>_brightness	-5 ~ 5	4/4	Preview of adjusting brightness of image according to mode settings.
c<0~(n-1)>_saturation	-5 ~ 5	4/4	Preview of adjusting saturation of image according to mode settings.
c<0~(n-1)>_contrast	-5 ~ 5	4/4	Preview of adjusting contrast of image according to mode settings.
c<0~(n-1)>_sharpness	-3 ~ 3	4/4	Preview of adjusting sharpness of image according to mode settings.
videoin_whitebalance	auto, manual	4/4	Preview of adjusting white balance of image according to mode settings
videoin_restoreatwb	0, 1~	4/4	Restore of adjusting white balance of image according to mode settings
videoin_exposurelevel	1 ~ 8	4/4	Preview of adjusting exposure level
videoin_agc	normal, max	4/4	Preview of adjusting agc
videoin_enableblc	0 ~ 1	4/4	Preview of adjusting enableblc

Group: **motion_c<0~(n-1)>** for n channel product

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	< oolean>	4/4	enable motion detection
win_i<0~2>_enable	< oolean>	4/4	enable motion window 1~3
win_i <0~2>_name	string[14]	4/4	name of motion window 1~3
win_i <0~2>_left	0 ~ 320	4/4	Left coordinate of window position.
win_i <0~2>_top	0 ~ 240	4/4	Top coordinate of window position.
win_i <0~2>_width	0 ~ 320	4/4	Width of motion detection window.
win_i<0~2>_height	0 ~ 240	4/4	Height of motion detection window.

win_i<0~2>_objsize	0 ~ 100	4/4	Percent of motion detection window.
win_i<0~2>_sensitivity	0 ~ 100	4/4	Sensitivity of motion detection window.

Group: **ddns**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	6/6	Enable or disable the dynamic dns.

provider	Safe100,
	DyndnsDynamic,
	DyndnsCustom,
	TZO,
	DHS,
	DynInterfree,
	CustomSafe100
		6/6	Safe100 => safe100.net
			DyndnsDynamic => dyndns.org (dynamic)
			DyndnsCustom => dyndns.org (custom)
			TZO => tzo.com
			DHS => dhs.org
			DynInterfree =>dyn-interfree.it
			CustomSafe100 =>
			Custom server using safe100 method

<provider>_hostname	string[128]	6/6	Your dynamic hostname.
<provider>_usernameemail	string[64]	6/6	Your user or email to login ddns service provider
<provider>_passwordkey	string[64]	6/6	Your password or key to login ddns service provider
<provider>_servername	string[128]	6/6	The server name for safe100. (This field only exists for provider is customsafe100)

Group: **upnppresentation**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	6/6	Enable or disable the UPNP presentation service.

Group: **upnpportforwarding**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	6/6	Enable or disable the UPNP port forwarding service.
upnpnatstatus	0~3	6/7	The status of UpnP port forwarding, used internally. 0 is OK, 1 is FAIL, 2 is no IGD router, 3 is no need to do port forwarding

Group: **syslog**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enableremotelog	<boolean>	6/6	enable remote log
serverip	<IP address>	6/6	Log server IP address
serverport	514, 1025~65535	6/6	Server port used for log
level	0~7	6/6	The levels to distinguish the importance of information. 0: LOG_EMERG 1: LOG_ALERT 2: LOG_CRIT 3: LOG_ERR 4: LOG_WARNING 5: LOG_NOTICE 6: LOG_INFO 7: LOG_DEBUG

Group: **camctrl_c<0~(n-1)>** for n channel product (capability.ptzenabled)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
panspeed	-5 ~ 5	1/4	Pan speed
tiltspeed	-5 ~ 5	1/4	Tilt speed
zoomspeed	-5 ~ 5	1/4	Zoom speed
autospeed	1 ~ 5	1/4	Auto pan/patrol speed
defaulthome	0 ~ 1	1/4	0: user define home 1: default home
returnhome	0 ~ 1	1/4	Enable return home position while idle.
returnhomeinterval	1~999	1/4	Time span for idle duration
axisx	-8250 ~ 8250	1/7	Axis X coordinate, used internally
axisy	-560 ~ 1664	1/7	Axis Y coordinate, used internally
axisz	0 ~ 780	1/7	Axis Z coordinate, used internally
preset_i<0~19>_name	string[40]	1/4	The name of preset location
preset_i<0~19>_pan	-8250 ~ 8250	1/4	The axis x coordinate of each preset location
preset_i<0~19>_tilt	-560 ~ 1664	1/4	The axis y coordinate of each preset location
preset_i<0~19>_zoom	0 ~ 780	1/4	The axis z coordinate of each preset location
patrol_i<0~39>_name	string[40]	1/4	The name of patrol location

patrol_i<0~39>_ dwelling	0 ~ 999	1/4	Time to dwelling of patrol location

Group: **layout**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
logo_default	<boolean>	1/6	0 => Custom logo 1 => Default logo
logo_link	string[40]	1/6	Hyperlink of the logo
theme_option	1~4	1/6	1~3: One of the default themes 4: Custom definition
theme_color_font	string[7]	1/6	Font color
theme_color_configfont	string[7]	1/6	Font color of configuration area
theme_color_titlefont	string[7]	1/6	Font color of video title
theme_color_controlbackground	string[7]	1/6	Background color of control area
theme_color_configbackground	string[7]	1/6	Background color of configuration area
theme_color_videobackground	string[7]	1/6	Background color of video area
theme_color_case	string[7]	1/6	Frame color

Group: **capability**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
api_httpversion	0200a	0/7	The HTTP API version.
bootuptime	<positive integer>	0/7	The server bootup time
nir	0, <positive integer>	0/7	number of IR interface
npir	0, <positive integer>	0/7	number of PIR
ndi	0, <positive integer>	0/7	number of digital input
ndo	0, <positive integer>	0/7	number of digital output
naudioin	0, <positive integer>	0/7	number of audio input

naudioout	0, <positive integer>	0/7	number of audio output
nvideoin	<positive integer>	0/7	number of video input
nmediastream	<positive integer>	0/7	number of media stream per channel
nvideosetting	<positive integer>	0/7	number of video settings per channel
naudiosetting	<positive integer>	0/7	number of audio settings per channel
nuart	0, <positive integer>	0/7	number of UART interface
ptzenabled	< positive integer >	0/7	An 32-bits integer, each bit can be set separately as follows: Bit 0 => Support camera control function 0(not support), 1(support) Bit 1 => Build-in or external camera. 0(external), 1(build-in) Bit 2 => Support pan operation. 0(not support), 1(support) Bit 3 => Support tilt operation. 0(not support), 1(support) Bit 4 => Support zoom operation. 0(not support), 1(support) Bit 5 => Support focus operation. 0(not support), 1(support) Bit 6 => Support iris operation. 0(not support), 1(support) Bit 7 => External or build-in PT. 0(build-in), 1(external) Bit 8 => Invalidate bit 1 ~ 7. 0(bit 1 ~ 7 are valid), 1(bit 1 ~ 7 are invalid) Bit 9 => Reserved bit; Invalidate lens_pan, Lens_tilt, lens_zoon, lens_focus, len_iris. 0(fields are valid), 1(fields are invalid)
lens_pan	<positive integer>	0/7	An 32-bits integer, each bit can be set separately as follows: Bit 0 => support pan Bit 1 => support pan in UI

			Bit 2 => External or build-in pan function. 0(build-in), 1(external)
lens_tilt	<positive integer>	0/7	An 32-bits integer, each bit can be set separately as follows: Bit 0 => support tilt Bit 1 => support tilt in UI Bit 2 => External or build-in tilt function. 0(build-in), 1(external)
lens_zoom	<positive integer>	0/7	An 32-bits integer, each bit can be set separately as follows: Bit 0 => support zoom Bit 1 => support zoom in UI Bit 2 => External or build-in zoom function. 0(build-in), 1(external)
lens_focus	<positive integer>	0/7	An 32-bits integer, each bit can be set separately as follows: Bit 0 => support focus Bit 1 => support focus in UI Bit 2 => External or build-in focus function. 0(build-in), 1(external) Bit 3 => support auto focus in UI
lens_iris	<positive integer>	0/7	An 32-bits integer, each bit can be set separately as follows: Bit 0 => support iris Bit 1 => support iris in UI Bit 2 => External or build-in iris function. 0(build-in), 1(external) Bit 3 => support auto iris in UI
npreset	<positive integer>	0/7	number of preset locations
protocol_https	< boolean >	0/7	indicate whether to support http over SSL
protocol_rtsp	< boolean >	0/7	indicate whether to support rtsp
protocol_sip	<boolean>	0/7	indicate whether to support sip
protocol_maxconnection	<positive integer>	0/7	The maximum allowed simultaneous connections
protocol_rtp_multicast_ scalable	<boolean>	0/7	indicate whether to support scalable multicast

protocol_rtp_multicast_ backchannel	<boolean>	0/7	indicate whether to support backchannel multicast
protocol_rtp_tcp	<boolean>	0/7	indicate whether to support rtp over tcp
protocol_rtp_http	<boolean>	0/7	indicate whether to support rtp over http
protocol_spush_mjpeg	<boolean>	0/7	indicate whether to support server push motion jpeg
protocol_snmp	<boolean>	0/7	indicate whether to support snmp
videoin_type	0, 1, 2	0/7	0 => Interlaced CCD 1 => Progressive CCD 2 => CMOS
videoin_resolution	<a list of the available resolution separates by comma)	0/7	available resolutions list
videoin_codec	<a list of the available codec types separaters by comma)	0/7	available codec list
videoout_codec	<a list of the available codec types separaters by comma)	0/7	available codec list
audio_aec	<boolean>	0/7	indicate whether to support acoustic echo cancellation
audio_extmic	<boolean>	0/7	indicate whether to support external microphone input
audio_linein	<boolean>	0/7	indicate whether to support external line input
audio_lineout	<boolean>	0/7	indicate whether to support line output
audio_headphoneout	<boolean>	0/7	indicate whether to support headphone output
audioin_codec	<a list of the available codec types separaters by comma)	0/7	available codec list
audioout_codec	<a list of the	0/7	available codec list

	available codec types separaters by comma)		
uart_httptunnel	<boolean>	0/7	Indicate whether to support the http tunnel for uart transfer
camctrl_privilege	<boolean>	0/7	Indicate whether to support “Manage Privilege” of PTZ control in Security page
transmission_mode	Tx, Rx, Both	0/7	Indicate what kind of transmission mode the machine used. TX: server, Rx: receiver box, Both: DVR?.
network_wire	<boolean>	0/7	Indicate whether to support the Ethernet
network_wireless	<boolean>	0/7	Indicate whether to support the wireless
wireless_802dot11b	<boolean>	0/7	Indicate whether to support the wireless 802.11b+
wireless_802dot11g	<boolean>	0/7	Indicate whether to support the wireless 802.11g
wireless_encrypt_wep	<boolean>	0/7	Indicate whether to support the wireless WEP
wireless_encrypt_wpa	<boolean>	0/7	Indicate whether to support the wireless WPA
wireless_encrypt_wpa2	<boolean>	0/7	Indicate whether to support the wireless WPA2
derivative_brand	<boolean>	0/7	Indicate whether to support upgrade function for the derivative brand. For example, if the value is true, the VVTK product can be upgraded to VVXX. (TCVV<->TCXX is excepted)
evctrlchannel	<boolean>	0/7	Indicate whether to support the http tunnel for event/control transfer
joystick	<boolean>	0/7	Indicate whether to support the joystick control

Group: **event_i<0~2>**

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
name	string[40]	6/6	The identification of this entry
enable	0, 1	6/6	To enable or disable this event.

priority	0, 1, 2	6/6	Indicate the priority of this event. "0" indicates low priority. "1" indicates normal priority. "2" indicates high priority.
delay	1~999	6/6	Delay seconds before detect next event.
trigger	boot, di, motion, seq,	6/6	Indicate the trigger condition. "boot" indicates system boot. "di" indicates digital input. "motion" indicates video motion detection. "seq" indicates periodic condition
di	<integer>	6/6	Indicate which di detected. This field is required when trigger condition is "di". One bit represents one digital input. The LSB indicates DI 0.
mdwin	<integer>	6/6	Indicate which motion detection windows detected. This field is required when trigger condition is "md". One bit represents one window. The LSB indicates the 1st window. For example, to detect the 1st and 3rd windows, set mdwin as 5.
inter	1~999	6/6	Interval of period snapshot in minute. This field is used when trigger condition is "seq".
weekday	<interger>	6/6	Indicate which weekday is scheduled. One bit represents one weekday. The bit0 (LSB) indicates Saturday. The bit1 indicates Friday. The bit2 indicates Thursday. The bit3 indicates Wednesday. The bit4 indicates Tuesday. The bit5 indicates Monday. The bit6 indicates Sunday. For example, to detect events on Friday and Sunday, set weekday as 66.
begintime	hh:mm	6/6	Begin time of weekly schedule.
endtime	hh:mm	6/6	End time of weekly schedule. (00:00 ~ 24:00 means always.)

action_do_i<0~(ndo-1)>_enable	0, 1	6/6	To enable or disable trigger digital output.
action_do_i<0~(ndo-1)>_duration	1~999	6/6	The duration of digital output is triggered in seconds.
action_goto_enable	0,1	6/6	To enable or disable event goto function
action_goto_name	string[40]	6/6	The selected name of preset positions
action_server_i<0~4>_enable	0, 1	6/6	To enable or disable this server action. The default value is 0.
action_server_i<0~4>_media	NULL, 0~4	6/6	The index of attached media.
action_server_i<0~4>__datefolder	<boolean>	6/6	Enable or disable create folders by date time and hour automatically

Group: **server_i<0~4>**

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
name	string[40]	6/6	The identification of this entry
type	email, ftp, http, ns	6/6	Indicate the server type. “email” is email server. “ftp” is ftp server. “http” is http server. “ns” is network storage.
http_url	string[128]	6/6	The url of http server to upload.
http_username	string[64]	6/6	The username to login in the server.
http_passwd	string[64]	6/6	The password of the user.
ftp_address	string[128]	6/6	The ftp server address
ftp_username	string[64]	6/6	The username to login in the server.
ftp_passwd	string[64]	6/6	The password of the user.
ftp_port	0~65535	6/6	The port to connect the server.
ftp_location	string[128]	6/6	The location to upload or store the media.
ftp_passive	0, 1	6/6	To enable or disable the passive mode. 0 is to disable the passive mode. 1 is to enable the passive mode.
email_address	string[128]	6/6	The email server address
email_username	string[64]	6/6	The username to login in the server.

email_sslmode	0, 1	6/6	Enable support SSL
email_port	0~65535	6/6	The port to connect the server.
email_passwd	string[64]	6/6	The password of the user.
email_senderemail	string[128]	6/6	The email address of sender.
email_recipientemail	string[128]	6/6	The email address of recipient.
ns_location	string[128]	6/6	The location to upload or store the media.
ns_username	string[64]	6/6	The username to login in the server.
ns_passwd	string[64]	6/6	The password of the user.
ns_workgroup	string[64]	6/6	The workgroup for network storage.

Group: **media_i<0~4>**(media_freespace is used internally.)

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
name	string[40]	6/6	The identification of this entry
type	snapshot, systemlog videoclip	6/6	The media type to send to the server or store by the server.
snapshot_source	<integer>	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and etc.
snapshot_prefix	string[16]	6/6	Indicate the prefix of the filename.
snapshot_datesuffix	0, 1	6/6	To add date and time suffix to filename or not. 1 means to add date and time suffix. 0 means not to add it.
snapshot_preevent	0 ~ 7	6/6	It indicates the number of pre-event images.
snapshot_postevent	0 ~ 7	6/6	The number of post-event images.
videoclip_source	<integer>	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and etc.
videoclip_prefix	string[16]	6/6	Indicate the prefix of the filename.
videoclip_preevent	0 ~ 9	6/6	It indicates the time of pre-event recording in seconds.
videoclip_maxduration	1 ~ 10	6/6	The time of maximum duration of one video clip in seconds.
videoclip_maxsize	50 ~ 1500	6/6	The maximum size of one video clip file in Kbytes.

Group: **recording_i**<0~1>

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
name	string[40]	6/6	The identification of this entry
enable	0, 1	6/6	To enable or disable this recoding.
priority	0, 1, 2	6/6	Indicate the priority of this recoding. "0" indicates low priority. "1" indicates normal priority. "2" indicates high priority.
source	<integer>	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and etc.
weekday	<interger>	6/6	Indicate which weekday is scheduled. One bit represents one weekday. The bit0 (LSB) indicates Saturday. The bit1 indicates Friday. The bit2 indicates Thursday. The bit3 indicates Wednesday. The bit4 indicates Tuesday. The bit5 indicates Monday. The bit6 indicates Sunday. For example, to detect events on Friday and Sunday, set weekday as 66.
begintime	hh:mm	6/6	Begin time of weekly schedule.
endtime	hh:mm	6/6	End time of weekly schedule. (00:00~24:00 means always.)
prefix	string[16]	6/6	Indicate the prefix of the filename.
limitsize	0,1	6/6	0: Entire free space mechanism 1: Limit recording size mechanism
cyclesize	30~	6/6	The maximum size for cycle recording in Kbytes when choose limit recording size.
cyclic	0,1	6/6	0: Disable cyclic recording 1: Enable cyclic recording
notify	0,1	6/6	0: Disable recording notification 1: Enable recording notification

notifyserver	0~31	6/6	Indicate which notification server is scheduled. One bit represents one application server (server_i0~i4). The bit0 (LSB) indicates server_i0. The bit1 indicates server_i1. The bit2 indicates server_i2. The bit3 indicates server_i3. The bit4 indicates server_i4. For example, enable server_i0, server_i2 and server_i4 to be notification server. The notifyserver value is 21.
reserveamount	15~	6/6	The reserve amount in Mbytes when choose cyclic recording mechanism.
dest	0~4	6/6	The destination to store the recording data. “0~4” means the index of network storage.

Group: **path**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
encoder1_start	<boolean>	7/7	Specify the http push server is active for stream 1
encoder2_start	<boolean>	7/7	Specify the http push server is active for stream 2

Group: **https** (product dependent)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
connect	1025 ~ 65535	7/7	Specify the stunnel connect port
enable	<boolean>	6/6	To enable or disable this secure http
policy	<Boolean>	6/6	If the value is 1, it will force http connection redirect to https connection

method	auto,
	manual,
	install
		6/6	auto => Create self-signed certificate automatically
			manual => Create self-signed certificate manually
			install => Create certificate request and install

status	-2 ~ 1	6/6	Specify the https status. -2=>invalid public key -1=>waiting for certificated 0=>not installed

			1=>active
countryname	string[2]	6/6	country name in certificate information
stateorprovincename	string[128]	6/6	state or province name in in certificate information
localityname	string[128]	6/6	the locality name in certificate information
organizationname	string[64]	6/6	organization naem in certificate information
unit	string[32]	6/6	organizational unit name in certificate information
commonname	string[64]	6/6	common name in certificate information
validdays	0 ~ 9999	6/6	certificatation valid period

Drive the digital output

Note: This request requires the privilege of viewer.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/dido/setdo.cgi?do1=<state>[&do2=<state>]
[&do3=<state>][&do4=<state>][&return=<return page>]
```

Where state is 0, 1. “0” means inactive or normal state while “1” means active or triggered state.

PARAMETER	VALUE	DESCRIPTION
do<num>	0, 1	0 – inactive, normal state
		1 – active, triggered state
return	*<return page>*	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according the the current path. If you omit this parameter, it will redirect to an empty page.

Example: Drive the digital output 1 to triggered state and redirect to an empty page

http://myserver/cgi-bin/dido/setdo.cgi?do1=1

Query status of the digital input

Note: This request requires the privilege of viewer.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/dido/getdi.cgi?[di0][&di1][&di2][&di3]
```

If no parameter is specified, all the status of digital input will be returned.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <length>\r\n
\r\n
[di0=<state>]\r\n
[di1=<state>]\r\n
[di2=<state>]\r\n
[di3=<state>]\r\n
```

where <*state*> can be 0 or 1.

Example: Query the status of digital input 1

```
Request:
http://myserver/cgi-bin/dido/getdi.cgi?di1

Response:
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: 7\r\n
\r\n
di1=1\r\n
```

Query status of the digital output

Note: This request requires the privilege of viewer.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/dido/getdo.cgi?[do0][&do1][&do2][&do3]
```

If no parameter is specified, all the status of digital output will be returned.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <length>\r\n
\r\n
[do0=<state>]\r\n
[do1=<state>]\r\n
[do2=<state>]\r\n
[do3=<state>]\r\n
```

where <*state*> can be 0 or 1.

Example: Query the status of digital output 1

Request:

http://myserver/cgi-bin/dido/getdo.cgi?do1

Response:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: 7\r\n
\r\n
do1=1\r\n
```

Capture single snapshot

Note: This request require normal user privilege

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/viewer/video.jpg?[channel=<value>][&resolution=<value>]
[&quality=<value>]
```

If the user requests the size larger than all stream setting on the server, this request will failed!

PARAMETER	VALUE	DEFAULT	DESCRIPTION
channel	0~(n-1)	0	the channel number of video source
resolution	*<available resolution>*	0	The resolution of image
quality	*1~5*	3	The quality of image

Server will return the most up-to-date snapshot of selected channel and stream in JPEG format. The size and quality of image will be set according to the video settings on the server.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: image/jpeg\r\n
[Content-Length: <image size>\r\n]

<binary JPEG image data>
```

Account management

Note: This request requires administrator privilege

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/admin/editaccount.cgi?
method=<value>&username=<name>[&userpass=<value>][&privilege=<value>]
[&privilege=<value>][…][&return=<return page>]
```

PARAMETER	VALUE	DESCRIPTION
method	Add	Add an account to server. When using this method, "username" field is necessary. It will use default value of other fields if not specified.
	Delete	Remove an account from server. When using this method, "username" field is necessary, and others are ignored.
	edit	Modify the account password and privilege. When using this method, "username" field is necessary, and other fields are optional. If not specified, it will keep original settings.
username	<name>	The name of user to add, delete or edit
userpass	<value>	The password of new user to add or that of old user to modify. The default value is an empty string.
privilege	<value>	The privilege of user to add or to modify.
	viewer	viewer's privilege
	operator	operator's privilege
	admin	administrator's privilege

return	<return page>	Redirect to the page *<return page>* after the parameter is assigned*.* The *<return page>* can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

System logs

Note: This request require administrator privilege

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/admin/syslog.cgi
```

Server will return the up-to-date system log.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <syslog length>\r\n
\r\n
<system log information>\r\n
```

Upgrade firmware

Note: This request requires administrator privilege

Method: POST

Syntax:

```
http://<servername>/cgi-bin/admin/upgrade.cgi
```

Post data:

```
fimage=<file name>[&return=<return page>]\r\n
\r\n
<multipart encoded form data>
```

Server will accept the upload file named <file name> to be upgraded the firmware and return with <return page> if indicated.

Camera Control

Note: This request requires privilege of viewer

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/camctrl/camctrl.cgi? [&move=<value>]
[&speedpan=<value>][&speedtilt=<value>][&speedzoom=<value>]
[&speedapp=<value>][&auto=<value>][&zoom=<value>][&zooming=<value>]
[&vx=<value>&vy=<value>&vs=<value>] [&return=<return page>]
```

PARAMETER	VALUE	DESCRIPTION
move	home	Move to camera to home position
	up	Move camera up
	down	Move camera down
	left	Move camera left
	right	Move camera right
speedpan	-5 ~ 5	Set the pan speed
speedtilt	-5 ~ 5	Set the tilt speed
speedzoom	-5 ~ 5	Set the zoom speed
speedapp	1 ~ 5	Set the auto pan/patrol speed
auto	pan	Auto pan
	patrol	Auto patrol
	stop	Stop camera
zoom	wide	To zoom for larger view with current speed
	tele	To zoom for farer view with current speed
	stop	To stop zoom
zooming	wide	To zoom without stop for larger view with current speed
	tele	To zoom without stop for farer view with current speed
vx	<integer , excluding 0>	The slope of movement = vy/vx, used for joystick control.

vy	<integer>	
vs	0 ~ 7	Set the speed of movement, "0" means stop.
return	<return page>	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

Recall

Note: This request requires privilege of viewer

Method: GET

Syntax:

```
http://<servername>/cgi-bin/camctrl/recall.cgi?
recall=<value> [&return=<return page>]
```

PARAMETER	VALUE	DESCRIPTION
recall	Text string less than 30 characters	One of the present positions to recall.
return	*<return page>*	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

System Information

Note: This request requires normal user privilege (obsolete)

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/sysinfo.cgi
```

Server will return the system information. In HTTP API version 2, the CapVersion will be 0200. All the fields in the previous version (0100) is obsolete. Please use "getparam.cgi?capability" instead.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <system information length>\r\n
\r\n
Model=<model name of server>\r\n
CapVersion=0200\r\n
```

PARAMETER(supported capability version)	VALUE	DESCRIPTION
Model	system.firmwareversion	Model name of server. Ex:IP3133-VVTK-0100a
CapVersion	*MMmm, MM is major version from 00 ~ 99* *mm is minor version from 00 ~ 99* *ex: 0100*	The capability field version

Preset Locations

Note: This request requires operator privilege

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/operator/preset.cgi?
[&addpos=<value>][&delpos=<value>][&return=<return page>]
```

PARAMETER	VALUE	DESCRIPTION
addpos	<Text string less than 30 characters>	Add one preset location to preset list.
delpos	<Text string less than 30 characters>	Delete preset location from preset list.
return	*<return page>*	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

IP filtering

Note: This request requires administrator access privilege

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/admin/ipfilter.cgi?
method=<value>&[start=<ipaddress>&end=<ipaddress>][&index=<value>]
[&return=<return page>]
```

PARAMETER	VALUE	DESCRIPTION
Method	addallow	Add a set of allow IP address range to server. Start and end parameters must be specified. If the index parameter is specified, it will try to add starting from index position.
	adddeny	Add a set of deny IP address range to server. Start and end parameters must be specified. If the index parameter is specified, it will try to add starting from index position.
	deleteallow	Remove a set of allow IP address range from server. If start and end parameters are specified, it will try to remove the matched IP address. If index is specified, it will try to remove the address from given index position. [start, end] parameters have higher priority then the [index] parameter.
	deletedeny	Remove a set of deny IP address range from server. If start and end parameters are specified, it will try to remove the matched IP address. If index is specified, it will try to remove the address from given index position. [start, end] parameters have higher priority then the [index] parameter.
start	<ip address>	The start IP address to add or to delete.
end	<ip address>	The end IP address to add or to delete.
index	<value>	The start position to add or to delete.
return	<return page>	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

Get SDP of Streamings

Note: This request requires viewer access privilege

Method: GET/POST

Syntax:

```
http://<servername>/<network_rtsp_s<0~m-1>_accessname>
```

“m” is the stream number.

“network_accessname_<0~(m-1)>” is the accessname for stream “1” to stream “m”. Please refer to the “subgroup of network: rtsp” for setting the accessname of SDP.

You can get the SDP by HTTP GET method.

Open the network streamings

Note: This request requires viewer access privilege

Syntax:

For http push server (mjpeg):

```
http://<servername>/<network_http_s<0~m-1>_accessname>
```

For rtsp (mp4), user needs to input the url below for a rtsp compatible player.

```
rtsp://<servername>/<network_rtsp_s<0~m-1>_accessname>
```

“m” is the stream number.

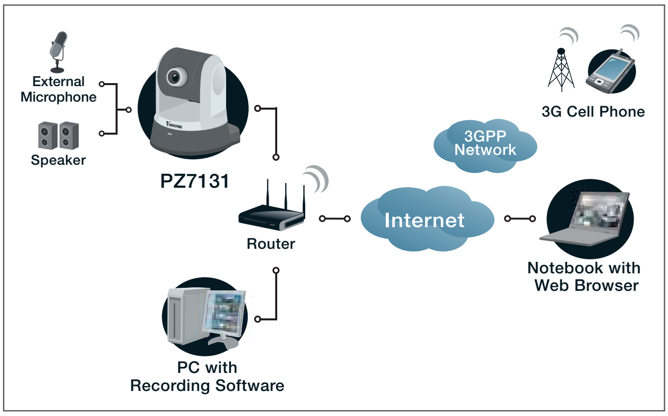
For detailed streaming protocol, please refer to “control signaling” and “data format” documents.

Technical Specifications

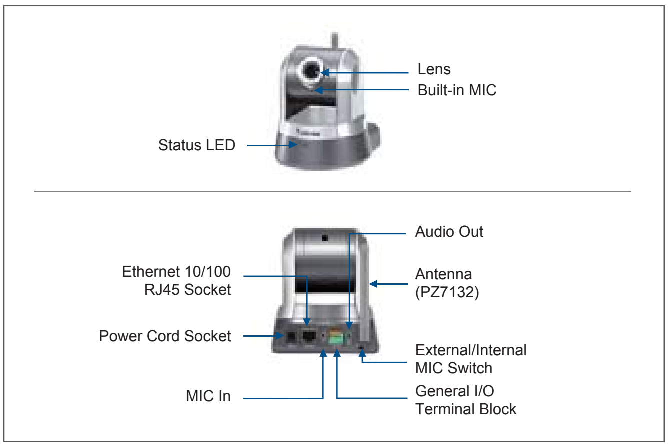
System	· CPU: VVTK-1000 SoC · Flash: 8 MB · RAM: 64 MB · Embedded OS: Linux 2.4
Pan/Tilt/Zoom	· Pan range: 350° (+175° ~ -175°) · Tilt range: 125° (+90° ~ -35°) · 2.6x optical zoom · Auto pan mode · Auto patrol mode
Lens	· Board lens, 2.6x optical zoom, f=2.8 ~ 7.3 mm, F1.9, auto-iris,focus range: 0.75 mm to infinity
Angle of View	· 28.7° ~ 73.4° (horizontal) · 21.6° ~ 54.7° (vertical) · 35.8° ~ 92.2° (diagonal)
Shutter Time	· 1/5 sec. to 1/15,000 sec.
Image sensor	· Micron 1/4" CMOS sensor in VGA resolution
Minimum Illumination	· 1.25 Lux / F1.9
Video	· Compression: MJPEG & MPEG-4 · Streaming: Simultaneous dual-streaming MPEG-4 streaming over UDP, TCP, HTTP, or HTTPS MPEG-4 multicast streaming MJPEG streaming over HTTP or HTTPS · Supports 3GPP mobile surveillance · Frame rates: MPEEG-4: Up to 30/25 fps at 640x480 MJPEG: Up to 30/25 fps at 640x480
Image Settings	· Adjustable image size, quality, and bit rate · Time stamp and text caption overlay · Flip & mirror · Configurable brightness, saturation contrast, sharpness and white balance · AGC, AES · Backlight Compensation (BLC)
Audio	· Compression: GSM-AMR speech encoding, bit rate: 4.75 kbps to 12.2 kbps MPEG-4 AAC audio encoding, bit rate: 16 kbps to 128 kbps · Interface: Built-in microphone External microphone input External audio output External/Internal microphone switch · Supports two-way audio by SIP protocol · Supports audio mute
Networking	· 10/100 Mbps Ethernet, RJ-45 · Protocols: IPv4, TCP/IP, HTTP, HTTPS, UPnP, RTSP/RTP/RTCP, IGMP, SMTP, FTP, DHCP, NTP, DNS, DDNS, and PPPoE · Built-in 802.11b/g WLAN (PZ7132)
Alarm and Event Management	· Triple-window video for motion detection · One D/I and one D/O for external sensor and alarm · Event notification using HTTP, SMTP, or FTP · Local recording of MP4 file
Security	· Multi-level user access with password protection · IP address filtering · HTTPS encrypted data transmission · Wireless: WEP, WPA-PSK, WPA2 (PZ7132)
Users	· Camera live viewing for up to 10 clients
Dimension	· 103.5 mm (D) x 104.1 mm (W) x 118 mm (H)
Weight	· Net: 352 g (PZ7131) · Net: 371 g (PZ7132)
LED Indicator	· System power and status indicator · System activity and network link indicator
Power	· 12V DC · Power consumption: Max. 12 W · 802.3af compliant Power over Ethernet (PZ7131)

Approvals	· CE, LVD, FCC, VCCI, C-Tick
Operating Environments	· Temperature: 0 ~ 50° C (32 ~ 122° F) · Humidity: 20% ~ 80% RH
Viewing System Requirements	· OS: Microsoft Windows 2000/XP/Vista · Browser: Internet Explorer 6.x or above · Cellphone: 3GPP player · Real Player: 10.5 or above · Quick Time: 6.5 or above
Installation, Management, and Maintenance	· Installation Wizard 2 · 16-CH recording software · Supports firmware upgrade
Applications	· SDK available for application development and system integration
Warranty	· 24 months

System Overview



External View


Lens
Built-in MIC
Status LED
Audio Out
Ethernet 10/100 RJ45 Socket
Antenna (PZ7132)
Power Cord Socket
External/Internal MIC Switch
MIC In
General I/O Terminal Block

Accessories

Enclosure

Mounting Kit

PoE Injector

All specifications are subject to change without notice. Copyright©2008 VIVOTEK INC. All rights reserved.

Technology License Notice

MPEG-4 AAC Technology

THIS PRODUCT IS LICENSED UNDER THE MPEG-4 AAC AUDIO PATENT LICENSE. THIS PRODUCT MAY NOT BE DECOMPILED, REVERSE-ENGINEERED OR COPIED, EXCEPT REGARD TO PC SOFTWARE, YOU MAY MAKE SINGLE COPIES FOR ARCHIVAL PURPOSES. FOR MORE INFORMATION, PLEASE REFER TO HTTP://WWW.VIALICENSING.COM.

MPEG-4 Visual Technology

THIS PRODUCT IS LICENSED UNDER THE MPEG-4 VISUAL PATENT PORTFOLIO LICENSE FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER FOR (i) ENCODING VIDEO IN COMPLIANCE WITH THE MPEG-4 VISUAL STANDARD ("MPEG-4 VIDEO") AND/OR (ii) DECODING MPEG-4 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED BY MPEG LA TO PROVIDE MPEG-4 VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION INCLUDING THAT RELATING TO PROMOTIONAL, INTERNAL AND COMMERCIAL USES AND LICENSING MAY BE OBTAINED FROM MPEG LA, LLC. PLEASE REFER TO HTTP://WWW.MPEGLA.COM.

AMR-NB Standard

THIS PRODUCT IS LICENSED UNDER THE AMR-NB STANDARD PATENT LICENSE AGREEMENT. WITH RESPECT TO THE USE OF THIS PRODUCT, THE FOLLOWING LICENSORS' PATENTS MAY APPLY:

TELEFONAKIEBOLAGET ERICSSON AB: US PAT. 6192335; 6275798; 6029125; 6424938; 6058359. NOKIA CORPORATION: US PAT. 5946651; 6199035. VOICEAGE CORPORATION: AT PAT. 0516621; BE PAT. 0516621; CA PAT. 2010830; CH PAT. 0516621; DE PAT. 0516621; DK PAT. 0516621; ES PAT. 0516621; FR PAT. 0516621; GB PAT. 0516621; GR PAT. 0516621; IT PAT. 0516621; LI PAT. 0516621; LU PAT. 0516621; NL PAT. 0516621; SE PAT 0516621; US PAT 5444816; AT PAT. 819303/AT E 198805T1; AU PAT. 697256; BE PAT. 819303; BR PAT. 9604838-7; CA PAT. 2216315; CH PAT. 819303; CN PAT. ZL96193827.7; DE PAT. 819303/DE69611607T2; DK PAT. 819303; ES PAT. 819303; EP PAT. 819303; FR PAT. 819303; GB PAT. 819303; IT PAT. 819303; JP PAT. APP. 8-529817; NL PAT. 819303; SE PAT. 819303; US PAT. 5664053. THE LIST MAY BE UPDATED FROM TIME TO TIME BY LICENSORS AND A CURRENT VERSION OF WHICH IS AVAILABLE ON LICENSOR'S WEBSITE AT HTTP://WWW.VOICEAGE.COM.

Electromagnetic Compatibility (EMC)

This device compiles with FCC Rules Part 15. Operation is subject to the following two conditions.

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

USA - This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a partial installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Shielded interface cables must be used in order to comply with emission limits.

Europe CE – This digital equipment fulfills the requirement for radiated emission according to limit B of EN55022/1998, and the requirement for immunity according to EN50082-1/1992.

Liability

VIVOTEK Inc. cannot be held responsible for any technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice. VIVOTEK Inc. makes no warranty of any kind with regard to the material contained within this document, including, but not limited to, the implied warranties of merchantability and fitness for any particular purpose.